



ŒUVRES COMPLÈTES

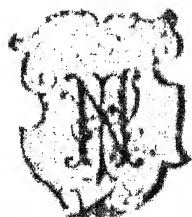
DE

THOMAS JAN STIEFELT

ÉDITÉES PAR LES SOUS-DE LA

SOCIÉTÉ MATHÉMATIQUE D'AMSTERDAM

TOME I





ŒUVRES COMPLÈTES  
DE  
THOMAS JAN STIEL

PUBLIÉES PAR LES SOINS DE LA  
SOCIÉTÉ MATHÉMATIQUE D'AMSTERDAM

TOME I







## PRÉFACE.

---

Dans sa réunion du 30 avril 1910, la Société mathématique d'Amsterdam prit la résolution de publier une édition complète des Oeuvres scientifiques de son membre défunt le docteur ès sciences Thomas Jan Stieltjes. Après la belle publication de la Correspondance d'Hermite et de Stieltjes par M.M. B. Baillaud et H. Bourget, la Société tenait à témoigner, elle aussi, de sa haute admiration pour l'oeuvre de l'éminent géomètre qui, nous ne saurions l'oublier, avant de devenir Français, avait été notre compatriote.

L'exécution de ce projet fut confiée à une commission composée de M.M. W. Kapteyn, J. C. Kluyver et E. F. van de Sande Bakhuyzen, qui acceptèrent cette tâche avec empressement. Après avoir été autorisée par les rédactions des différents journaux à réimprimer les notes et mémoires en question, la commission demanda à M<sup>me</sup> Stieltjes la permission de consulter les papiers laissés par son époux, afin de pouvoir examiner s'il s'y trouvait encore quelque travail dans un état assez avancé pour en permettre la publication. M<sup>me</sup> Stieltjes ayant gracieusement acquiescé à cette demande, la commission a pu ajouter quelques petites notes au second volume de cette collection.

Les notes et mémoires avaient été publiés en diverses langues: dix en hollandais, deux en allemand, tous les autres en français. La commission décida de les réimprimer tous tels qu'ils étaient, en ajoutant une traduction française aux articles hollandais.

dont les N<sup>o</sup> 15 et 34 sont des traductions françaises des N<sup>o</sup> 15 et 34 respectivement. La suppression pure et simple de ces deux traductions a lieu à un changement de numérotage. Pour conserver, autant que possible les mêmes numéros, nous avons substitué au N<sup>o</sup> 15 l'article tiré de la Zeitschrift für Vermessungswesen (Stuttgart, 1881). Cet article fut envoyé de Paris au rédacteur de ce journal mais la commission est en possession d'une lettre qui se trouve dans le second volume et dont on peut tirer, presque avec certitude, que cet inconnu était Stieltjes. Cette substitution permet de continuer les numéros de la Notice jusqu'au N<sup>o</sup> 37. Mais à partir de là les numéros de l'édition présente sont devenus inférieurs d'une unité aux numéros de l'édition précédente. En outre quelques notes seront ajoutées à la fin du second volume. Elles indiqueront quelles sont les lettres de la Correspondance qui ont servi à différents articles, on y insérera les notes qui se trouvent dans la Correspondance de M. Cosserat et enfin la commission ajoutera encore elle-même quelques notes et éclaircissements.

La commission n'a pas jugé opportun de joindre aux Notices une notice biographique. Elle n'aurait pu que redire ce qui est dit et si bien dit dans la „Notice sur Stieltjes“ que M. Houzeau a publiée. La Correspondance; elle y a seulement joint un portrait datant de quelques années de Stieltjes.

# TABLE DES MATIÈRES.

---

- I. Iets over de benaderde voorstelling van eene functie door eene andere . . . . .
- I. De la représentation approximative d'une fonction par une autre. (traduction) . . . . .
- II. Een en ander over de integraal  $\int_0^1 \log \Gamma(x + u) du$  . . . . .
- II. Remarques sur l'intégrale  $\int_0^1 \log \Gamma(x + u) du$ . (traduction) . . . . .
- III. Notiz über einen elementaren Algorithmus . . . . .
- IV. Over Lagrange's Interpolatieformule . . . . .
- IV. A propos de la formule d'interpolation de Lagrange. (traduction) . . . . .
- V. Eenige opmerkingen omtrent de differentiaalquotienten van eene functie van één veranderlijke . . . . .
- V. Quelques remarques à propos des dérivées d'une fonction d'une seule variable. (traduction) . . . . .
- VI. Over eenige theorema's omtrent oneindige reeksen . . . . .
- VI. A propos de quelques théorèmes concernant les séries finies. (traduction) . . . . .
- VII. Over de transformatie van de periodieke functie  $A_0 + A_1 \cos \varphi + B_1 \sin \varphi + \dots + A_n \cos n \varphi + B_n \sin n \varphi$  . . . . .
- VII. De la transformation de la fonction périodique  $A_0 + A_1 \cos \varphi + B_1 \sin \varphi + \dots + A_n \cos n \varphi + B_n \sin n \varphi$  (traduction) . . . . .
- VIII. Over een algorithmus voor het meetkundig midden . . . . .
- VIII. Sur un algorithme de la moyenne géométrique. (traduction) . . . . .

- XII. Sur un théorème de M. Tisserand. (Note présentée par M. Hermite) . . . . .
- XIII. Bewijs van de stelling, dat eene geheele rationele functie altijd, voor zekere reële of complexe waarden van de veranderlijke, de waarde nul aanneemt . . . . .
- XIII. Preuve du théorème, d'après lequel une fonction rationnelle et rationnelle s'annule pour certaines valeurs réelles ou complexes de la variable. (traduction) . . . . .
- XIV. Quelques considérations sur la fonction rationnelle d'une variable complexe . . . . .
- XV. Möglichkeit oder Unmöglichkeit einer Potenzenstimmung . . . . .
- XVI. Sur la théorie des résidus biquadratiques (Extrait d'une Lettre adressée à M. Hermite) . . . . .
- XVII. Sur le nombre des diviseurs d'un nombre entier (Note présentée par M. Hermite) . . . . .
- XVIII. Sur l'évaluation approchée des intégrales. (Note présentée par M. Hermite) . . . . .
- XIX. Sur l'évaluation approchée des intégrales. (Note présentée par M. Hermite) . . . . .
- XX. Sur quelques théorèmes arithmétiques. (Extrait d'une lettre adressée à M. Hermite) . . . . .
- XXI. Sur la décomposition d'un nombre en cinq carrés (Extrait d'une lettre adressée à M. Hermite) . . . . .
- XXII. Sur un théorème de Liouville. (Note présentée par M. Hermite) . . . . .
- XXIII. Sur un théorème de M. Liouville. (Note présentée par M. Hermite) . . . . .
- XXIV. Sur le nombre de décompositions d'un entier en cinq carrés (Extrait d'une lettre adressée à M. Hermite) . . . . .
- XXV. Over de quadratische ontbinding van priemgetallen in den vorm  $3n + 1$  . . . . .

	Page.
XXVIII. Sur le caractère du nombre 2 comme résidu ou non-résidu quadratique . . . . .	362
XXIX. Quelques remarques sur l'intégration d'une équation différentielle . . . . .	364
XXX. Note sur le problème du plus court crépuscule . . . . .	375
XXXI. Quelques recherches sur la théorie des quadratures dites mécaniques . . . . .	377
XXXII. Sur un développement en fraction continue. (Note présentée par M. Tisserand) . . . . .	395
XXXIII. Note sur la densité de la Terre . . . . .	397
XXXIV. Quelques remarques sur la variation de la densité dans l'intérieur de la Terre . . . . .	400
XXXV. Note sur quelques formules pour l'évaluation de certaines intégrales . . . . .	426
XXXVI. Sur une généralisation de la théorie des quadratures mécaniques. (Note présentée par M. Tisserand) . . . . .	428
XXXVII. Note à l'occasion de la réclamation de M. Markoff . . . . .	430
XXXVIII. Un théorème d'algèbre. (Extrait d'une Lettre adressée à M. Hermite) . . . . .	432
XXXIX. Sur certains polynômes qui vérifient une équation différentielle linéaire du second ordre et sur la théorie des fonctions de Lamé. . . . .	434
XL. Sur quelques théorèmes d'algèbre. (Note présentée par M. Hermite) . . . . .	440
XLI. Sur les polynômes de Jacobi. (Note présentée par M. Hermite) . . . . .	442
XLII. Sur une généralisation de la série de Lagrange . . . . .	445
XLIII. Sur l'intégrale $\int_0^{\infty} \frac{e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}}$ . . . . .	451
XLIV. Sur une fonction uniforme (Note présentée par M. Hermite) . . . . .	457
XLV. Sur une loi asymptotique dans la théorie des nombres.	



# I.

(Afzonderlijk gedrukt te Delft in 1876)

## Iets over de benaderde voorstelling van eene functie door eene andere.

Is de functie  $f(x)$  continu voor alle waarden van  $x$  tusschen  $a$  en  $b$  en zoo ook  $\varphi(x, a_1, a_2, \dots, a_n)$ , dan kan men de vraag stellen de constanten  $a_1, a_2, \dots, a_n$  zóó te bepalen, dat de functie  $\varphi(x)$  voor  $a < x < b$  zo weinig mogelijk van  $f(x)$  verschilt.

Het ligt voor de hand de constanten  $a_1, a_2, \dots, a_n$  te bepalen door de voorwaarden, dat voor

$$\left. \begin{array}{l} x = x_1, \\ x = x_2, \\ \dots\dots\dots \\ x = x_n \end{array} \right\} (a < x_1 < x_2 \dots < x_n < b).$$

de functie  $\varphi(x)$  dezelfde waarden aanneemt als  $f(x)$ , zoodat men heeft

$$\begin{aligned} (1) \quad & \dots\dots\dots f(x_p) = \varphi(x_p, a_1, a_2, \dots, a_n). \\ & (p = 1, 2, \dots, n) \end{aligned}$$

Door  $\varphi(x)$  in plaats van  $f(x)$  te nemen, maakt men eene fout

$$(2) \quad \dots\dots\dots R(x) = f(x) - \varphi(x),$$

eene continue functie van  $x$ , die nul wordt voor





$M$  is dus hier afhankelijk van  $x_1, x_2, \dots, x_n$ , evenals de grootheden  $a_1, a_2, \dots, a_n$  dit zijn ten gevolge van de vergelijkingen (1).

Maar men kan ook  $a_1, a_2, \dots, a_n$  als de onafhankelijk veranderlijken aannemen;  $x_1, x_2, \dots, x_n$  zijn dan de wortels van de vergelijking

$$f(x) = \varphi(x, a_1, a_2, \dots, a_n)$$

en kunnen als afhankelijk van  $a_1, a_2, \dots, a_n$  beschouwd worden. De condities voor een minimum van  $M$  zijn dan

$$\frac{\partial M}{\partial a_1} = 0,$$

$$\frac{\partial M}{\partial a_2} = 0,$$

$$\dots\dots\dots$$

$$\frac{\partial M}{\partial a_n} = 0,$$

of daar  $R(x)$  telkens aan de veranderlijke grenzen der integralen nu wordt

$$0 = \int_a^{x_1} \frac{\partial R(x)}{\partial a_p} dx - \int_{x_1}^{x_2} \frac{\partial R(x)}{\partial a_p} dx + \dots + (-1)^n \int_{x_n}^b \frac{\partial R(x)}{\partial a_p} dx,$$

( $p = 1, 2, \dots, n$ )

of wel, daar volgens (2)

$$-\frac{\partial R}{\partial a_p} = \frac{\partial \varphi}{\partial a_p}$$

is,

$$(3) \quad 0 = \int_a^{x_1} \frac{\partial \varphi(x)}{\partial a_p} dx - \int_{x_1}^{x_2} \frac{\partial \varphi(x)}{\partial a_p} dx + \dots + (-1)^n \int_{x_n}^b \frac{\partial \varphi(x)}{\partial a_p} dx.$$

( $p = 1, 2, \dots, n$ )

In (1) en (3) heeft men nu te zamen  $2n$  vergelijkingen ter bepaling van  $a_1, a_2, \dots, a_n, x_1, x_2, \dots, x_n$ .

$$\frac{\partial \varphi(x)}{\partial a_p}$$

want dan is

$$\frac{\partial \varphi(x)}{\partial a_p} = \varphi_p(x)$$

en de vergelijkingen (3) worden

$$(4) \quad 0 = \int_a^{x_1} \varphi_p(x) dx - \int_{x_1}^{x_2} \varphi_p(x) dx + \dots + (-1)^{p-1} \int_{x_{p-1}}^{x_p} \varphi_p(x) dx + (-1)^p \int_{x_p}^b \varphi_p(x) dx$$

$$(p = 1, 2, \dots, n)$$

waarin nu alleen  $x_1, x_2, \dots, x_n$  voorkomen. Men kan deze grootheden bepalen; ze hangen niet af van  $f(x)$ . Zij nu bekend, dan heeft men ter bepaling van  $a_1, a_2, \dots, a_n$  de vergelijkingen (1) op te lossen, die nu lineair worden, en

$$f(x_p) = a_1 \varphi_1(x_p) + a_2 \varphi_2(x_p) + \dots + a_n \varphi_n(x_p)$$

$$(p = 1, 2, \dots, n)$$

De uitdrukking voor  $M$  wordt eenvoudiger in plaats van

$$(b-a)M = \int_a^{x_1} \{f(x) - a_1 \varphi_1(x) - \dots - a_n \varphi_n(x)\} dx - \dots$$

$$\pm \int_{x_n}^b \{f(x) - a_1 \varphi_1(x) - \dots - a_n \varphi_n(x)\} dx$$

mag men volgens (4) schrijven

$$(b-a)M = \int_a^{x_1} f(x) dx - \int_{x_1}^{x_2} f(x) dx + \dots + (-1)^{n-1} \int_{x_{n-1}}^{x_n} f(x) dx + (-1)^n \int_{x_n}^b f(x) dx$$

Het eenvoudigste bijzondere geval is nu hier

$$\varphi_1(x) = 1,$$

$$\varphi_2(x) = x,$$

$$\varphi_3(x) = x^2,$$



dan wordt

$$0 = \int_0^{u_1} \psi(\cos u) \sin u \, du - \int_{u_1}^{u_2} \psi(\cos u) \sin u \, du + \dots + (-1)^{n-1} \int_{u_{n-1}}^{u_n} \psi(\cos u) \sin u \, du$$

Nu is

$$\frac{\sin pu}{\sin u} = 2^{p-1} \cos^{p-1} u - \dots$$

eene geheele rationale functie van  $\cos u$  van den  $p$ ten graden.  
mag dus stellen

$$\psi(\cos u) = \frac{\sin pu}{\sin u}$$

$$(p = 1, 2, \dots, n)$$

en vindt zoo

$$(7) \quad 0 = \int_0^{u_1} \sin pu \, du - \int_{u_1}^{u_2} \sin pu \, du + \dots + (-1)^{n-1} \int_{u_{n-1}}^{u_n} \sin pu \, du$$

$$(p = 1, 2, \dots, n)$$

of

$$0 = 2 \cos pu_1 - 2 \cos pu_2 + \dots + (-1)^{n-1} 2 \cos pu_n$$

$$(p = 1, 2, \dots, n)$$

Dat nu hieraan voldaan wordt door de waarde

$$u_1 = \frac{\pi}{n+1} = \alpha,$$

$$u_2 = \frac{2\pi}{n+1} = 2\alpha,$$

$$\dots \dots \dots$$

$$u_n = \frac{n\pi}{n+1} = n\alpha$$

blijkt gemakkelijk, want stelt men

$$P = 2 \cos pa - 2 \cos 2pa + 2 \cos 3pa - \dots + (-1)^{n-1} 2 \cos npa$$

dan volgt

Nu is

$$\sin(n+1)pa = \sin p\pi = 0$$

en

$$\sin npa = \sin(p\pi - pa) = (-1)^{p-1} \sin pa,$$

dus volgt, daar  $\sin pa$  niet nul kan zijn,

$$P = 1 + (-1)^{n+p-1}.$$

Voor  $n = 1$  kan dadelijk geverifieerd worden, dat  $u_1 = \frac{\pi}{2}$  aan (7) voldoet. Hiermee is dus de juistheid der in (6) gegeven waarden aangetoond. Er blijft nog over iets van de waarde van  $M$  te zeggen. Deze is bepaald door

$$2M = \int_{-1}^{x_1} f(x) dx - \dots + (-1)^n \int_{x_n}^1 f(x) dx.$$

Kan nu  $f(x)$  voor alle waarden van  $x$  tusschen  $-1$  en  $+1$  ontwikkeld worden in eene reeks

$$f(x) = b_0 + b_1x + b_2x^2 + \dots = \sum_{p=0}^{p=\infty} b_p x^p,$$

dan vallen bij de substitutie hiervan in de uitdrukking van  $2M$  de eerste termen weg, en er blijft

$$2M = \int_{-1}^{x_1} \sum_{p=0}^{p=\infty} b_{n+p} x^{n+p} dx - \dots + (-1)^n \int_{x_n}^1 \sum_{p=0}^{p=\infty} b_{n+p} x^{n+p} dx.$$

Neemt men nu hiervan alleen den eersten term om eene benaderde waarde  $S$  van  $M$  te vinden, dan is

$$2S = b_n \left\{ \int_{-1}^{x_1} x^n dx - \dots + (-1)^n \int_{x_n}^1 x^n dx \right\},$$

of ook

$$2S = (-1)^n b_n \left\{ \int_0^{u_1} [\cos^n u + \psi(\cos u)] \sin u \, du - \dots \right. \\ \left. + (-1)^n \int_{u_n}^{\pi} [\cos^n u + \psi(\cos u)] \sin u \, du \right\}$$

Men mag nu voor  $\cos^n u + \psi(\cos u)$  nemen

$$\frac{\sin(n+1)u}{2^n \sin u} = \cos^n u - \dots$$

en dan wordt na uitvoering der integratie

$$2S = \frac{(-1)^n b_n}{2^n(n+1)} \left\{ -2 \cos(n+1)u_1 + 2 \cos(n+1)u_2 - \dots \right. \\ \left. + (-1)^n 2 \cos(n+1)\pi \right\}$$

dus daar

$$(n+1)u_p = p\pi,$$

is

$$(8) \quad S = \frac{(-1)^n b_n}{2^n}.$$

Om een enkel voorbeeld te geven: laat gevraagd worden voor  $0 < y < 1$  benaderend door eene uitdrukking van de vorm  $a_1 + a_2 x$  voor te stellen.

Men neme hier eerst:

$$\sqrt{1 + \frac{1+x}{2}} = a_1 + a_2 x, \\ (-1 < x < +1)$$

dan is  $n = 2$ ,

$$x_1 = \cos \frac{2\pi}{3} = -\frac{1}{2},$$

$$x_2 = \cos \frac{\pi}{3} = +\frac{1}{2},$$

dus

$$\frac{1}{2} \sqrt{5} = a_1 - \frac{1}{2} a_2,$$

$$\frac{1}{2} \sqrt{7} = a_1 + \frac{1}{2} a_2,$$

of

$$a_1 = \frac{1}{4} (\sqrt{7} + \sqrt{5}),$$

$$\alpha = \frac{1}{4} [3\sqrt{5} - \sqrt{7}] = 1,0256 \dots,$$

$$\beta = \sqrt{7} - \sqrt{5} = 0,4097 \dots$$

Om de waarde van  $S$  te vinden, dient hier de ontwikkeling

$$\begin{aligned} \sqrt{1 + \frac{1+x}{2}} &= \sqrt{\frac{3}{2}} \sqrt{1 + \frac{x}{3}} \\ &= \sqrt{\frac{3}{2}} \left\{ 1 + \frac{x}{2 \cdot 3} - \frac{x^2}{8 \cdot 9} + \dots \right\}, \end{aligned}$$

us

$$b_2 = -\frac{\sqrt{6}}{144}$$

en

$$S = -\frac{\sqrt{6}}{576} = -0,00425 \dots$$

Overigens kan hier de waarde van  $M$  zelf gemakkelijk gevonden worden; ik vind

$$M = -0,00437 \dots$$

Dat hier aan de gestelde voorwaarden voldaan is, ligt voor de hand.

Ik merk nog op, dat de vergelijking (7) in verband met (4) doet zien, dat wanneer men eene functie  $f(x)$  voor  $0 < x < \pi$  benaderen wil voorstellen door

$$a_1 \sin x + a_2 \sin 2x + \dots + a_n \sin nx,$$

voor  $x_1, x_2, \dots, x_n$  de waarden

$$\frac{\pi}{n+1}, \frac{2\pi}{n+1}, \dots, \frac{n\pi}{n+1},$$

genomen moeten worden. Dit zijn juist de waarden voor welke Lagrange eene eenvoudige methode gegeven heeft om  $a_1, a_2, \dots, a_n$  te bepalen, namelijk de vergelijkingen (1) op te lossen. Het resultaat is



De grootheid  $M$  is hier

$$\pi M = \int_0^{\frac{\pi}{n+1}} f(x) dx - \dots + (-1)^n \int_{\frac{n\pi}{n+1}}^{\pi} f(x) dx$$

ze convergeert blijkbaar voor  $n = \infty$  tot nul, wanneer eene continue functie van  $x$  is.

# I.

(Brochure imprimée à Delft en 1876)  
(traduction)

---

## De la représentation approximative d'une fonction par une autre.

Les deux fonctions  $f(x)$  et  $\varphi(x, a_1, a_2, \dots, a_n)$  étant continues pour toutes les valeurs de  $x$  entre  $a$  et  $b$ , on peut se proposer de donner aux constantes  $a_1, a_2, \dots, a_n$  des valeurs telles que pour  $a < x < b$  la fonction  $\varphi(x)$  diffère de  $f(x)$  aussi peu que possible.

Il est clair que dans ce but on peut déterminer les constantes  $a_1, a_2, \dots, a_n$  par la condition que pour

$$\left. \begin{array}{l} x = x_1, \\ x = x_2, \\ \dots\dots\dots \\ x = x_n \end{array} \right\} (a < x_1 < x_2 < \dots < x_n < b)$$

la fonction  $\varphi(x)$  prenne les mêmes valeurs que  $f(x)$ , en sorte qu'on ait

$$(1) \quad \dots\dots\dots f(x_p) = \varphi(x_p, a_1, a_2, \dots, a_n)$$

pour toutes les valeurs  $p = 1, 2, \dots, n$ .

En prenant  $\varphi(x)$  au lieu de  $f(x)$  on commet une erreur

$$(2) \quad \dots\dots\dots R(x) = f(x) - \varphi(x).$$

$R(x)$  est une fonction continue de  $x$  qui s'annule pour

Supposons la courbe

$$y = R(x) = f(x) - \varphi(x)$$

construite; d'après ce que nous venons de dire elle est  
aux  $n$  points

$$x = x_1,$$

$$x = x_2,$$

$$\dots\dots\dots$$

$$x = x_n,$$

$$y = 0.$$

La concordance des fonctions  $f(x)$  et  $\varphi(x)$  est bonne si la courbe  $y = R(x)$  s'éloigne peu de l'axe des  $X$  pour  $a < x < b$ . Pour un nombre  $n$  des grandeurs  $x_1, x_2, \dots, x_n$  on peut obtenir une approximation de  $\varphi(x)$  avec  $f(x)$ ; mais, si le nombre  $n$  est grand, l'approximation qu'on peut atteindre dépend du choix des  $x_1, x_2, \dots, x_n$ . Nous examinerons maintenant quel est le choix le plus convenable.

A cet effet, il est nécessaire de dire ce qu'il faut entendre par le minimum des deux fonctions. Ici nous prendrons pour mesure l'écart la somme de toutes les aires comprises entre la courbe  $y = R(x)$  et les deux ordonnées extrêmes qui correspondent à  $x = a$  et à  $x = b$ ; toutes ces aires étant comptées de même signe. Nous représentons cette somme par

$$(b - a) M,$$

M est la moyenne arithmétique des erreurs entre  $x = a$  et  $x = b$ , les erreurs étant prises en valeur absolue. Il faudra donc choisir les grandeurs  $x_1, x_2, \dots, x_n$  de manière à rendre M minimum.

Dans l'hypothèse que  $R(x)$  change de signe toutes les fois qu'on passe par une des valeurs  $x_1, x_2, \dots, x_n$  et que  $R(x)$  ne s'annule pas pour aucune autre valeur de la variable entre  $a$  et  $b$ , on a

M dépend donc ici de  $x_1, x_2, \dots, x_n$ , de même que  $a_1, a_2, \dots, a_n$  en dépendent d'après les équations (1)

Mais on peut aussi prendre  $a_1, a_2, \dots, a_n$  comme variables indépendantes;  $x_1, x_2, \dots, x_n$  sont alors les racines de l'équation

$$f(x) = \varphi(x, a_1, a_2, \dots, a_n)$$

et peuvent être considérées comme dépendant de  $a_1, a_2, \dots, a_n$ . Les conditions pour que M soit minimum sont alors

$$\frac{\partial M}{\partial a_1} = 0,$$

$$\frac{\partial M}{\partial a_2} = 0,$$

$$\dots\dots\dots$$

$$\frac{\partial M}{\partial a_n} = 0,$$

ou bien, vu que  $R(x)$  s'annule toutes les fois aux limites variables des intégrales,

$$0 = \int_a^{x_1} \frac{\partial R(x)}{\partial a_p} dx - \int_{x_1}^{x_2} \frac{\partial R(x)}{\partial a_p} dx + \dots + (-1)^n \int_{x_n}^b \frac{\partial R(x)}{\partial a_p} dx.$$

( $p = 1, 2, \dots, n$ )

Mais suivant l'équation (2)

$$-\frac{\partial R}{\partial a_p} = \frac{\partial \varphi}{\partial a_p}.$$

Donc

$$0 = \int_a^{x_1} \frac{\partial \varphi(x)}{\partial a_p} dx - \int_{x_1}^{x_2} \frac{\partial \varphi(x)}{\partial a_p} dx + \dots + (-1)^n \int_{x_n}^b \frac{\partial \varphi(x)}{\partial a_p} dx.$$

( $p = 1, 2, \dots, n$ )

Les équations (1) et (3) qui sont au nombre de  $2n$ , peuvent servir à la détermination de  $a_1, a_2, \dots, a_n, x_1, x_2, \dots, x_n$ .

$$R(x) = \varphi(x, a_1, a_2, \dots, a_n) = 0$$

on obtient

$$0 = \int_0^{u_1} \psi(\cos u) \sin u \, du - \int_{u_1}^{u_2} \psi(\cos u) \sin u \, du + \dots + (-1)^n \int_{u_n}^{u_{n+1}} \psi(\cos u) \sin u \, du$$

Or

$$\frac{\sin pu}{\sin u} = 2^{p-1} \cos^{p-1} u - \dots$$

est une fonction de  $\cos u$  entière et rationnelle du  $\cos u$ , on peut donc poser

$$\psi(\cos u) = \frac{\sin pu}{\sin u}$$

$$(p = 1, 2, \dots, n)$$

et l'on trouve de cette façon

$$(7) \quad 0 = \int_0^{u_1} \sin pu \, du - \int_{u_1}^{u_2} \sin pu \, du + \dots + (-1)^n \int_{u_n}^{u_{n+1}} \sin pu \, du$$

$$(p = 1, 2, \dots, n)$$

ou

$$0 = 2 \cos pu_1 - 2 \cos pu_2 + \dots + (-1)^{n-1} 2 \cos pu_n$$

$$(p = 1, 2, \dots, n)$$

On voit aisément que les valeurs

$$u_1 = \frac{\pi}{n+1} = \alpha,$$

$$u_2 = \frac{2\pi}{n+1} = 2\alpha,$$

$$\dots$$

$$u_n = \frac{n\pi}{n+1} = n\alpha$$

satisfont à cette équation, car si l'on pose

$$P = 2 \cos pa - 2 \cos 2pa + 2 \cos 3pa - \dots + (-1)^n 2 \cos npa$$

il s'ensuit

Or on a

$$\sin (n+1) p a=\sin p \pi=0$$

et

$$\sin n p a=\sin (p \pi-p a)=(-1)^{p-1} \sin p a .$$

On conclut de là, vu que  $\sin p a$  ne peut pas être nul, que

$$P=1+(-1)^{n+p-1} .$$

Pour  $n=1$  on vérifie immédiatement que  $u_1=\frac{\pi}{2}$  satisfait à l'équation (7)

Il est donc démontré que les valeurs (6) satisfont au problème. Reste à parler de la valeur de  $M$ ; elle est

$$2 M=\int_{-1}^{x_1} f(x) d x-\ldots+(-1)^n \int_{x_n}^{+1} f(x) d x .$$

Lorsque  $f(x)$  pour toutes les valeurs de  $x$  entre  $-1$  et  $+1$  peut être développée en une série

$$f(x)=b_0+b_1 x+b_2 x^2+\ldots=\sum_{p=0}^{p=\infty} b_p x^p,$$

les  $n$  premiers termes de l'équation qui donne  $2 M$  disparaissent quand on y substitue cette valeur de  $f(x)$ . Il reste

$$2 M=\int_{-1}^{x_1} \sum_{p=0}^{p=\infty} b_{n+p} x^{n+p} d x-\ldots+(-1)^n \int_{x_n}^{+1} \sum_{p=0}^{p=\infty} b_{n+p} x^{n+p} d x .$$

Si nous prenons  $p=0$ , pour trouver une valeur approchée  $S$  de  $M$  nous avons

$$2 S=b_n\left\{\int_{-1}^{x_1} x^n d x-\ldots+(-1)^n \int_{x_n}^{+1} x^n d x\right\}$$

ou bien

$$2 S=b_n\left\{\int_{-1}^{x_1}[x^n+\psi(x)] d x-\ldots+(-1)^n \int_{x_n}^{+1}[x^n+\psi(x)] d x\right\},$$

$$2S = (-1)^n b_n \left\{ \int_0^{u_1} [\cos^n u + \psi(\cos u)] \sin u \, du - \dots \right. \\ \left. + (-1)^n \int_{u_n}^{\pi} [\cos^n u + \psi(\cos u)] \sin u \, du \right\}$$

Or, au lieu de  $\cos^n u + \psi(\cos u)$  on peut prendre

$$\frac{\sin(n+1)u}{2^n \sin u} = \cos^n u - \dots$$

et alors on trouve après l'intégration

$$2S = \frac{(-1)^n b_n}{2^n(n+1)} \left\{ -2 \cos(n+1)u_1 + 2 \cos(n+1)u_n \right. \\ \left. + (-1)^{n+1} \right\}$$

partant, comme

$$(n+1)u_p = p\pi,$$

$$(8) \quad \dots \quad S = \frac{(-1)^n b_n}{2^n}.$$

Considérons un seul exemple: on demande de développer  $\sqrt{1+y}$  pour  $0 < y < 1$  par une expression

Ici il faut prendre d'abord

$$\sqrt{1 + \frac{1+x}{2}} = a_1 + a_2 x. \\ (-1 < x < +1)$$

Alors  $n=2$ ,

$$x_1 = \cos \frac{2\pi}{3} = -\frac{1}{2},$$

$$x_2 = \cos \frac{\pi}{3} = +\frac{1}{2},$$

par conséquent

$$\frac{1}{2} \sqrt{5} = a_1 - \frac{1}{2} a_2,$$

$$\frac{1}{2} \sqrt{7} = a_1 + \frac{1}{2} a_2,$$

ou

$$a_1 = \frac{1}{4} (\sqrt{7} + \sqrt{5})$$

Donc

$$\alpha = \frac{1}{4} [3\sqrt{5} - \sqrt{7}] = 1,0256 \dots,$$

$$\beta = \sqrt{7} - \sqrt{5} = 0,4097 \dots$$

Pour trouver la valeur de S, on se sert du développement en série suivant :

$$\begin{aligned}\sqrt{1 + \frac{1+x}{2}} &= \sqrt{\frac{3}{2}} \sqrt{1 + \frac{x}{3}} \\ &= \sqrt{\frac{3}{2}} \left\{ 1 + \frac{x}{2 \cdot 3} - \frac{x^2}{8 \cdot 9} + \dots \right\}.\end{aligned}$$

Donc

$$b_2 = -\frac{\sqrt{6}}{144}$$

$$S = -\frac{\sqrt{6}}{576} = -0,00425 \dots$$

D'ailleurs la valeur précise de M peut aisément être calculée dans ce cas. Je trouve

$$M = -0,00437 \dots$$

Il est évident que les conditions posées sont satisfaites.

J'observe encore que l'équation (7) jointe à l'équation (4) fait voir qu'il faut que si l'on veut approximativement représenter une fonction  $f(x)$  par

$$\begin{aligned}a_1 \sin x + a_2 \sin 2x + \dots + a_n \sin nx, \\ (0 < x < \pi)\end{aligned}$$

il faut prendre pour  $x_1, x_2, \dots, x_n$  les valeurs

$$\frac{\pi}{n+1}, \quad \frac{2\pi}{n+1}, \quad \dots, \quad \frac{n\pi}{n+1}.$$

Ce sont là précisément les valeurs pour lesquelles Lagrange a donné une méthode simple permettant de déterminer  $a_1, a_2, \dots, a_n$ , c. à d. comment résoudre les équations (1). Le résultat est le suivant :



La grandeur  $M$  est ici donnée par l'équation

$$\pi M = \int_0^{\frac{\pi}{n+1}} f(x) dx - \dots + (-1)^n \int_{\frac{n\pi}{n+1}}^{\pi} f(x) dx$$

Pour  $n = \infty$  elle converge évidemment vers zéro  
c'est ici le cas, est une fonction continue de  $x$ .

## II.

(Amsterdam, Nieuw Arch. Wisk., 4, 1878, 100—104.)

---

Een en ander over de integraal  $\int_0^1 \log \Gamma(x+u) du$ .

In het volgende zal ik laten zien, dat de waarde van deze integraal gevonden kan worden door onmiddellijke toepassing van de gewone definitie van eene bepaalde integraal, en daaraan eenige opmerkingen toevoegen over eene functie, waarvan de afgeleide van  $\log \Gamma(x)$  een bijzonder geval is.

De waarde van de bovenstaande integraal is bekend, en wel is<sup>1</sup>

$$(1) \quad \int_0^1 \log \Gamma(x+u) du = \frac{1}{2} \log 2\pi + x \log x - x.$$

Hierin wordt  $x$  positief ondersteld; als uiterste waarde kan  $x=0$  zijn, dan is

$$(2) \quad \int_0^1 \log \Gamma(u) du = \frac{1}{2} \log 2\pi.$$

In deze laatste integraal wordt  $\log \Gamma(u)$  voor  $u=0$  oneindig, maar uit

$$\int_0^1 \log \Gamma(u) du = \int_0^1 \log \Gamma(u+1) du - \int_0^1 \log u du$$

ziet men, dat de integraal toch eene eindige waarde heeft, en welk die waarde is; want de eerste integraal rechts is volgens (1) gelijk aan  $\frac{1}{2} \log 2\pi - 1$ , en de tweede is gelijk aan  $-1$ .

Ik onderstel nu  $x$  positief, en ga uit van de bekende formules

Om echter te zien wat hierbij uit het tweede lid v  
eenige andere eigenschappen van de functie  $\psi(x, p)$

Uit de als definitie gestelde formule (7) volgt o

$$\psi(x+1, p) = \psi(x, p) + \frac{1}{x^p},$$

en algemeener

$$(9) \quad \psi(x+k, p) = \psi(x, p) + \frac{1}{x^p} + \frac{1}{(x+1)^p} + \dots + \frac{1}{(x+k-1)^p}$$

Uit deze laatste formule blijkt, dat (7) ook aldus gesch

$$\psi(x, p) = \lim_{n \rightarrow \infty} \left( \frac{n^{1-p} - 1}{1-p} - \psi(x+n, p) \right) + \psi(x, p)$$

of

$$0 = \lim_{n \rightarrow \infty} \left( \frac{n^{1-p} - 1}{1-p} - \psi(x+n, p) \right),$$

waarvoor men verder mag schrijven

$$0 = \lim_{n \rightarrow \infty} \left( \frac{(x+n)^{1-p} - 1}{1-p} - \psi(x+n, p) \right),$$

want het verschil

$$\frac{(x+n)^{1-p} - 1}{1-p} - \frac{n^{1-p} - 1}{1-p}$$

convergeert voor  $n \rightarrow \infty$  tot nul. Voor  $p > 1$  en vo  
dit dadelijk, en wanneer  $p$  tusschen 0 en 1 ligt,

$$\frac{(x+n)^{1-p} - 1}{1-p} - \frac{n^{1-p} - 1}{1-p} = \int_0^{x+n} \frac{du}{u^p} - \int_0^n \frac{du}{u^p} = \int_n^{x+n} \frac{du}{u^p}$$

( $0 < \theta < 1$ )

Vervangt men nu nog  $n+x$  door  $x$ , dan volgt

$$(10) \quad \dots \dots \lim_{x \rightarrow \infty} \left( \frac{x^{1-p} - 1}{1-p} - \psi(x, p) \right) = 0.$$

Is nu  $x$  positief en  $0 < p \leq 1$ , dan volgt hieruit voor  $k = \infty$ , op (10) lettende

$$(11) \quad \dots \int_0^1 \psi(x+u, p) du = \frac{x^{1-p} - 1}{1-p}.$$

$$(x > 0, 0 < p \leq 1)$$

Stelt men in de formule, waaruit dit door grensovergang afgeleid werd,  $x = \frac{1}{k}$  en daarna  $k = \infty$ , dan blijkt, dat de formule (11) ook nog geldt voor  $x = 0$ .

Uit deze formule (11) ontstaat nu voor  $p = 1$  de formule (6).

Ik eindig met eenige verdere opmerkingen omtrent de functie  $\psi(x, p)$ .

Is  $x$  positief, dan kan  $\psi(x, p)$  door eene bepaalde integraal uitgedrukt worden

$$(12) \quad \dots \quad \psi(x, p) = \frac{1}{\Gamma(p)} \int_0^\infty \left( \frac{1}{u} - \frac{e^{-(x-1)u}}{1-e^{-u}} \right) e^{-xu} u^{p-1} du,$$

waaruit men weder verdere ontwikkelingen kan afleiden, bijv.

$$(13) \quad \dots \quad \psi(x, p) = \psi(1, p) + \frac{1}{\Gamma(p)} \int_0^1 \frac{1-u^{x-1}}{1-u} \left( \log \frac{1}{u} \right)^{p-1} du,$$

$$(14) \quad \psi(x, p) = \frac{x^{1-p} - 1}{1-p} - \frac{1}{2x^p} - \frac{1}{\Gamma(p)} \int_0^\infty \left( \frac{1}{1-e^{-u}} - \frac{1}{u} - \frac{1}{2} \right) e^{-xu} u^{p-1} du$$

Men kan namelijk, wanneer  $x$  positief is, de formule (7) herleiden door  $\frac{1}{x^p}$ ,  $\frac{1}{(x+1)^p}$  enz. als bepaalde integralen te schrijven van den vorm

$$\frac{1}{a^p} = \frac{1}{\Gamma(p)} \int_0^\infty u^{p-1} e^{-au} du,$$

en eveneens de eerste term

$$\frac{n^{1-p} - 1}{1-p} = \frac{1}{\Gamma(p)} \int_0^\infty \frac{e^{-u} - e^{-nu}}{u} u^{p-1} du.$$

Deze laatste formule ontstaat uit de voorafgaande, door met  $da$  te vermenigvuldigen, en tusschen de grenzen  $a=1$  en  $a=n$  te integreeren

## II.

(Amsterdam, Nieuw Arch. Wisk., 4, 1878  
(traduction)

### Remarques sur l'intégrale $\int_0^1 \log \Gamma(x)$

Je me propose de faire voir ici, que la valeur de  
être trouvée par une application immédiate de la  
de l'intégrale définie. J'ajouterai quelques remarques  
fonction qui dans un cas particulier se réduit à la

La valeur de l'intégrale écrite ci-dessus est connue

$$(1) \quad \dots \int_0^1 \log \Gamma(x+u) du = \frac{1}{2} \log 2\pi + x \log x -$$

Dans ces expressions  $x$  a par hypothèse une valeur

Dans ce dernier cas on a

$$(2) \quad \dots \int_0^1 \log \Gamma(u) du = \frac{1}{2} \log 2\pi.$$

Pour  $u=0$ , l'expression  $\log \Gamma(u)$  qui figure dans l'intégrale  
devient infinie, mais la formule

$$\int_0^1 \log \Gamma(u) du = \int_0^1 \log \Gamma(u+1) du - \int_0^1 \log$$

montre que cette intégrale a néanmoins une valeur finie  
de cette formule. En effet, la première intégrale  
vaut  $\frac{1}{2} \log 2\pi - 1$  d'après la formule (1), et la seconde

Je suppose maintenant  $x$  positif et je pars de

La formule (4) donne le développement ordinaire de  $\log \Gamma(x)$  en une série semi-convergente, limitée aux premiers termes.

Il résulte de (3)

$$\begin{aligned} 5) \quad \frac{1}{n} \left[ \log \Gamma(x) + \log \Gamma\left(x + \frac{1}{n}\right) + \dots + \log \Gamma\left(x + \frac{n-1}{n}\right) \right] = \\ = \left( \frac{1}{2} - \frac{1}{2n} \right) \log 2\pi - \left( x - \frac{1}{2n} \right) \log n + \frac{1}{n} \log \Gamma(nx). \end{aligned}$$

Pour  $n = \infty$  le premier membre devient

$$\int_0^1 \log \Gamma(x+u) du,$$

et la limite du second membre est aisément trouvée à l'aide de (4).

Je commence par traiter le cas  $x = \frac{1}{n}$ . Dans ce cas spécial la formule (3) peut être déduite beaucoup plus facilement que dans le cas général: il suffit alors d'employer la formule

$$\Gamma(x) \Gamma(1-x) = \frac{\pi}{\sin \pi x}.$$

Au lieu de (5) on trouve alors

$$\frac{1}{n} \left[ \log \Gamma\left(\frac{1}{n}\right) + \log \Gamma\left(\frac{2}{n}\right) + \dots + \log \Gamma\left(\frac{n}{n}\right) \right] = \left( \frac{1}{2} - \frac{1}{2n} \right) \log 2\pi - \frac{1}{2n} \log n$$

et pour  $x = \infty$  on obtient la formule (2).

Dans le cas général le second membre de (5) devient d'après la formule (4)

$$\begin{aligned} \left( \frac{1}{2} - \frac{1}{2n} \right) \log 2\pi - \left( x - \frac{1}{2n} \right) \log n + \frac{1}{2n} \log 2\pi + \left( x - \frac{1}{2n} \right) \log nx - x + \frac{\theta}{12n^2x} = \\ = \frac{1}{2} \log 2\pi + \left( x - \frac{1}{2n} \right) \log x - x + \frac{\theta}{12n^2x} \end{aligned}$$

et pour  $n = \infty$  on trouve la formule (1).

En différentiant la formule (1) par rapport à  $x$ , on trouve

$$6) \quad \dots \dots \dots \int_0^1 \psi(x+u) du = \log x,$$

où l'on a posé

L'hypothèse  $x=0$  ou  $x=1$  peut servir à la détermination de la constante  $C$ , si l'on suppose la formule (2) connue. La dernière, elle peut être trouvée assez facilement, ce qui sera fait remarquer plus haut.

La formule (6) est un cas particulier d'une formule plus générale. En effet, si l'on prend une fonction  $\psi(x, p)$ , définie par

$$(7) \quad \psi(x, p) = \lim_{n \rightarrow \infty} \left\{ \frac{n^{1-p} - 1}{1-p} - \frac{1}{x^p} - \frac{1}{(x+1)^p} - \dots - \frac{1}{(x+n-1)^p} \right\}$$

( $p > 0, x > 0$ )

ce qui pour  $p=1$  prend la forme

$$\psi(x, 1) = \lim_{n \rightarrow \infty} \left\{ \log n - \frac{1}{x} - \frac{1}{x+1} - \dots - \frac{1}{x+n-1} \right\}$$

et, pour  $p > 1$ , la forme

$$\psi(x, p) = \frac{1}{p-1} - \frac{1}{x^p} - \frac{1}{(x+1)^p} - \frac{1}{(x+2)^p} - \dots$$

il est aisé de voir que  $\psi(x, p)$  a réellement une valeur finie. La fonction  $\psi(x, 1)$  est identique à celle que nous avons désignée plus haut par  $\psi(x)$ .

Il n'est pas même nécessaire de supposer tout d'abord qu'on ait affaire à des fonctions réelles; dans l'équation (7) par exemple,  $x$  peut fort bien devenir négatif.

Lorsque  $k$  est un nombre entier positif, il s'en suit que

$$\begin{aligned} & \psi(x, p) + \psi\left(x + \frac{1}{k}, p\right) + \psi\left(x + \frac{2}{k}, p\right) + \dots + \psi\left(x + \frac{k-1}{k}, p\right) \\ &= \lim_{n \rightarrow \infty} k^p \left\{ \frac{(nk)^{1-p} - 1}{1-p} - \frac{1}{(kx)^p} - \frac{1}{(kx+1)^p} - \dots - \frac{1}{(kx+k-1)^p} \right\} \end{aligned}$$

ou

$$(8) \quad \psi(x, p) + \psi\left(x + \frac{1}{k}, p\right) + \dots + \psi\left(x + \frac{k-1}{k}, p\right) = k^p \psi\left(x, \frac{p}{k}\right)$$

ce qui apparaît immédiatement, si dans (7) on remplace  $x$  par  $x + \frac{r}{k}$ .

Mais avant d'examiner ce que devient alors le second membre, je dois commencer par établir quelques autres propriétés de la fonction  $\psi(x, p)$ .

De la formule (7) qui définit la fonction  $\psi(x, p)$ , on tire immédiatement

$$\psi(x+1, p) = \psi(x, p) + \frac{1}{x^p},$$

et plus généralement

$$(9) \quad \psi(x+k, p) = \psi(x, p) + \frac{1}{x^p} + \frac{1}{(x+1)^p} + \dots + \frac{1}{(x+k-1)^p}.$$

Cette dernière formule fait voir qu'au lieu de (7) on peut également écrire

$$\psi(x, p) = \lim_{n=\infty} \left( \frac{n^{1-p} - 1}{1-p} - \psi(x+n, p) + \psi(x, p) \right),$$

ou

$$0 = \lim_{n=\infty} \left( \frac{n^{1-p} - 1}{1-p} - \psi(x+n, p) \right).$$

Cette dernière équation peut être remplacée par

$$0 = \lim_{n=\infty} \left( \frac{(x+n)^{1-p} - 1}{1-p} - \psi(x+n, p) \right).$$

En effet, la différence

$$\frac{(x+n)^{1-p} - 1}{1-p} - \frac{n^{1-p} - 1}{1-p}$$

converge vers zéro pour  $n = \infty$ . On le voit immédiatement pour  $p > 1$  et pour  $p = 1$ ; lorsque  $p$  est entre 0 et 1, la vérité de cette proposition ressort du calcul suivant:

$$\frac{(x+n)^{1-p} - 1}{1-p} - \frac{n^{1-p} - 1}{1-p} = \int_0^{x+n} \frac{du}{u^p} - \int_0^n \frac{du}{u^p} = \int_n^{x+n} \frac{du}{u^p} = \frac{x}{(n+\theta x)^p},$$

$$(0 < \theta < 1)$$

En remplaçant encore  $n+x$  par  $x$ , on en tire

$$(10) \quad \lim_{n \rightarrow \infty} \left( \frac{x^{1-p} - 1}{1-p} - \psi(x, p) \right) = 0$$



Si l'on suppose  $x$  positif et  $0 < p \leq 1$ , il s'ensuit d'après la formule (10),

$$(11) \quad \dots \int_0^1 \psi(x+u, p) du = \frac{x^{1-p} - 1}{1-p}.$$

$(x > 0, 0 < p \leq 1)$

La formule (11) est valable aussi pour  $x=0$ ; il faut poser  $x = \frac{1}{k}$ , et ensuite  $k = \infty$  dans la formule (10). Nous venons de dériver la formule (11) en passant de (10) à (11).

Or, pour  $p=1$ , la formule (11) se transforme en

Je termine en faisant encore quelques remarques sur la fonction  $\psi(x, p)$ .

Lorsque  $x$  est positif,  $\psi(x, p)$  peut être exprimé en fonction de la fonction  $\Gamma(p)$  définie

$$(12) \quad \dots \psi(x, p) = \frac{1}{\Gamma(p)} \int_0^\infty \left( \frac{1}{u} - \frac{e^{-(x-1)u}}{1-e^{-u}} \right) e^{-u} u^{p-1} du$$

d'où l'on peut tirer entre autres les développements

$$(13) \quad \dots \psi(x, p) = \psi(1, p) + \frac{1}{\Gamma(p)} \int_0^1 \frac{1-u^{x-1}}{1-u} \left( \log \frac{1}{u} \right) u^{p-1} du$$

$$(14) \quad \psi(x, p) = \frac{x^{1-p} - 1}{1-p} - \frac{1}{2x^p} - \frac{1}{\Gamma(p)} \int_0^\infty \left( \frac{1}{1-e^{-u}} - \frac{1}{u} \right) e^{-u} u^{p-1} du$$

En effet, lorsque  $x$  est positif, on peut réduire la formule (12) en écrivant  $\frac{1}{x^p}$ ,  $\frac{1}{(x+1)^p}$ , etc. sous forme d'intégrales de la forme

$$\frac{1}{a^p} = \frac{1}{\Gamma(p)} \int_0^\infty u^{p-1} e^{-au} du.$$

On a de même pour le premier terme

$$\frac{x^{1-p} - 1}{1-p} = \frac{1}{\Gamma(p)} \int_0^\infty \frac{e^{-u} - e^{-xu}}{u} u^{p-1} du$$

Cette dernière formule se tire de l'avant-dernière en multipliant celle-ci par  $da$  et qu'on intègre entre les limites  $a=1$  et  $a=x$ .

### III.

(J. Math., Berlin, 89, 1880, 343—344.)

---

#### Notiz über einen elementaren Algorithmus.

Es seien  $a_1, a_2, \dots, a_k$  reelle Zahlen,  $M_1$  ihr arithmetisches Mittel,  $M_2$  das arithmetische Mittel aller Producte aus je zwei verschiedenen dieser Zahlen,  $M_3$  das arithmetische Mittel aller Producte aus je drei verschiedenen dieser Zahlen u. s. w. Die letzte der auf diese Weise zu bildenden Grössen ist  $M_k = a_1 a_2 \dots a_k$ . Es soll ferner festgesetzt werden  $M_0 = 1$ .

Im Allgemeinen ist dann

$$\begin{aligned} M_p^2 - M_{p-1} M_{p+1} \\ (p = 1, 2, \dots, k-1) \end{aligned}$$

positiv; genauer gefasst: dieser Ausdruck wird nie negativ und nur dann gleich Null, wenn entweder sämtliche Zahlen  $a_1, a_2, \dots, a_k$  einander gleich sind, oder wenn mindestens  $k-p+1$  dieser Zahlen gleich Null sind. Im letzteren Falle ist offenbar  $M_p = M_{p+1} = 0$ . Sind jetzt die Zahlen  $a_1, a_2, \dots, a_k$  sämtlich positiv und setzt man

$$\begin{aligned} a'_p &= \frac{M_p}{M_{p-1}}, \\ (p &= 1, 2, \dots, k) \end{aligned}$$

und wenn von den Zahlen  $a_1, a_2, \dots, a_k$  keine  $> a_1$

$$a'_1 = \frac{a_1 + a_2 + \dots + a_k}{k} \leq \frac{(k-1)a_1 + a_k}{k}$$

$$a'_k = \frac{k}{\frac{1}{a_1} + \frac{1}{a_2} + \dots + \frac{1}{a_k}} > a_k,$$

folglich:

$$0 < a'_1 - a'_k < \frac{k-1}{k} (a_1 - a_k).$$

Durch wiederholte Anwendung der Operation  
Zahlen  $a'_1, a'_2, \dots, a'_k$  aus  $a_1, a_2, \dots, a_k$  hergeleitet wurde  
Gruppen von  $k$  Zahlen, deren Product unverändert  
sie sich unbegrenzt einander nähern Die Zahlen

convergiren also sämmtlich gegen die Grenze ( $a$ )

Bezeichnet man die Zahlen der  $n^{\text{ten}}$  abgeleitet

$$a_p^{(n)},$$

$$(p = 1, 2, \dots, k)$$

so werden die Differenzen

$$a_p^{(n)} - a_{p+1}^{(n)},$$

$$(p = 1, 2, \dots, k-1)$$

welche sich beliebig der Null nähern, immer mehr  
sodass das Verhältniss von je zwei dieser Differenzen  
für  $n = \infty$  die Einheit zur Grenze hat.

## IV.

(Amsterdam, Versl. K. Akad. Wet., 1<sup>e</sup> sect., sér. 2, 17,  
1882, 239—254.)

---

### Over Lagrange's Interpolatieformule.

1. De gewoonlijk aldus genoemde formule leert de geheele rationale functie van  $x$ , van den  $n - 1^{\text{sten}}$  graad hoogstens, die voor de  $n$  bijzondere waarden  $x = x_1, x = x_2, \dots, x = x_n$  met eene willekeurige functie  $f(x)$  in waarde overeenkomt, onder den volgende vorm kennen

$$\sum_{p=1}^{p=n} \frac{\varphi(x)}{(x-x_p)\varphi'(x_p)} f(x_p),$$

waarin

$$\varphi(x) = (x-x_1)(x-x_2)\dots(x-x_n)$$

en  $\varphi'(x)$  als gewoonlijk, de afgeleide functie van  $\varphi(x)$  voorstelt.

Is de functie  $f(x)$  zelf geheel rationaal, van niet hooger dan den  $n - 1^{\text{sten}}$  graad, dan is identiek

$$f(x) = \sum_{p=1}^{p=n} \frac{\varphi(x)}{(x-x_p)\varphi'(x_p)} f(x_p).$$

In het algemeen echter moet deze formule aangevuld worden door eene rest, evenals dit bij het theorema van Taylor het geval is.

ledige rest van de reeks van Taylor voorstelt Lagrange<sup>1)</sup> kan afleiden, kan men ook een analoge interpolatieformule van Lagrange uit de veelvuldige afgeleiden, waaronder Hermite de rest voorstelt afleiden. Veeltijds deze vereenvoudigde rest bij de reeks van Taylor zonder van de hulpmiddelen der integraalrekening af te kunnen, kan men hetzelfde ook voor den analogen rest van de Hermite'sche interpolatieformule verlangen. Eene zoodanige ontwerping is in het volgende gegeven.

Ik merk nog op dat, hoewel de hier verkregen rest uit Hermite's formule afgeleid kan worden, de vereenvoudigden restvorm gegeven heeft. Het is een elementaire eigenschap van bepaalde enkelvoudige en veelvoudige integralen uit te breiden, wat echter geen nood is.

De te bewijzen formule kan aldus geschreven worden

$$(1) \dots\dots f(x) = \sum_{p=1}^{p=n} \frac{\varphi(x)}{(x-x_p) \varphi'(x_p)} f(x_p) + \frac{\varphi(x)}{1 \cdot 2 \cdot \dots \cdot n} \dots$$

waarin  $\xi$  eene waarde heeft, gelegen tusschen de kleinste en de grootste der getallen  $x, x_1, \dots, x_n$ .

Hierbij moet ondersteld worden, dat de afgeleiden  $f'(z), f''(z), \dots, f^{n-1}(z)$  eindig en continu zijn voor alle  $z$  gelegen tusschen  $x, x_1, \dots, x_n$  en dat voor dezelfde  $z$  de functie  $f^{n-1}(z)$  een eindig en bepaald differentiaalcoëfficiënt heeft.

De formule (1) neemt een meer eleganten vorm aan, als men  $f^n(\xi)$  uit afzondert; men overtuigt zich gemakkelijk dat deze gedaante aanneemt

$$(2) \dots\dots \frac{f(x)}{\psi'(x)} + \frac{f(x_1)}{\psi'(x_1)} + \frac{f(x_2)}{\psi'(x_2)} + \dots + \frac{f(x_n)}{\psi'(x_n)} = \frac{f^n(\xi)}{1 \cdot 2 \cdot \dots \cdot n}$$

waarin

2. Het bewijs van de formule (1) berust nu op de volgende hulpstelling:

„Wanneer de functie  $G(z)$  voor de  $n+1$  verschillende waarden  $z = x, z = x_1, \dots, z = x_n$  de waarde nul aanneemt, dan neemt het  $n^{\text{de}}$  differentiaalquotiënt  $G^n(z)$  de waarde nul aan voor eene waarde  $z = \xi$  gelegen tusschen het grootste en het kleinste der getallen  $x, x_1, \dots, x_n$ .

Ondersteld wordt hierbij, dat  $G(z), G'(z), \dots, G^{n-1}(z)$  eindig en continu zijn voor alle waarden van  $z$  gelegen tusschen  $x, x_1, \dots, x_n$ , en dat voor dezelfde waarden van  $z$  de functie  $G^{n-1}(z)$  een eindig en bepaald differentiaalquotiënt  $G^n(z)$  heeft.

Voor  $n=1$  is dit een bekend theorema, waaromtrent het voldoende is te verwijzen naar Dini, *Fondamenti per la teoria delle funzioni di variabili reali*, p. 70.

Het bewijs van dit theorema, evenals dat van eenige nauw verwante, zooals het in de nog meest gangbare leerboeken voorkomt (bijv. Serret, *Cours de calcul différentiel et intégral*, bevat eene leemte die eerst aangevuld werd door eenige onderzoekingen van Weierstrass (zie Dini, p. 43—51. Weierstrass zelf schijnt van deze onderzoekingen omtrent de grondslagen der functieleer niets gepubliceerd te hebben).

Het is vooral noodig op te merken, dat in het eenvoudigste geval  $n=1$  de grootheid  $\xi$  tusschen  $x$  en  $x_1$  ligt, en verschillend zoowel van  $x$  als van  $x_1$  aangenomen mag worden.

Het bewijs van de hulpstelling in het algemeene geval volgt onmiddellijk uit de waarheid in het eenvoudigste geval  $n=1$ . Immers, namelijk  $n=2$ , dus

$$G(x)=0, \quad G(x_1)=0, \quad G(x_2)=0,$$

dan kan men onderstellen

$$x < x_1 < x_2$$

in het algemeene geval  $\xi$  ondersteld mag worden noch aan het grootste, noch aan het kleinste der  $g$ . De voorwaarden van continuïteit en differentieerbaarheid der functie  $G(z)$  en de afgeleide functies moet stellen, welke moeite uit die, welke voor het geval  $n = 1$  gesteld

3. Het bewijs van de formule (1) kan nu aldus

Ter bekorting moge het interpolatiepolynoom  $F(x)$  aangeduid worden, zoodat

$$(3) \quad \dots \dots F(x) = \sum_{p=1}^{p=n} \frac{\varphi(x)}{(x-x_p) \varphi'(x_p)} f(x_p).$$

Onder de waarden  $x_1, x_2, \dots, x_n$  komen geen twee daar de functiën  $F(x)$  en  $f(x)$  voor  $x = x_1, x = x_2, \dots$  waarden aannemen, en het ons te doen is om in het knoopen vorm van het verschil  $f(x) - F(x)$  te vinden hierbij zonder nadeel de onderstelling maken, dat  $x$  samenvalt met een der waarden  $x_1, x_2, \dots, x_n$ .

Dit aangenomen, zij

$$(4) \quad \dots \dots f(x) = F(x) + (x-x_1)(x-x_2)\dots(x-x_n).$$

De waarde van  $R$  is dan hierdoor volkomen bepaald. Verder, voor een oogenblik,  $x, x_1, \dots, x_n$  als constanten en  $z$  eene nieuwe veranderlijke is, beschouwen

$$(5) \quad \dots \dots G(z) = -f(z) + F(z) + (z-x_1)(z-x_2)\dots(z-x_n).$$

waarin dus  $R$  de door (4) volkomen bepaalde, waarde heeft.

Blijkbaar is nu, niet alleen

$$G(x) = 0,$$

maar ook

en is

$$G^n(z) = -f^n(z) + 1.2.3 \dots n.R.$$

Wegens (6) volgt nu

$$R = \frac{1}{1.2.3 \dots n} f^n(\xi)$$

en dit in (4) gesubstitueerd geeft

$$f(x) = F(x) + \frac{(x-x_1)(x-x_2)\dots(x-x_n)}{1.2.3 \dots n} f^n(\xi),$$

waarmede het bewijs van de formule (1) geleverd is.

4. Wanneer men in de nu ook bewezen formule (2) de steeds ongelijke getallen  $x, x_1, \dots, x_n$  allen tot eenzelfde limiet  $X$  laat convergeeren, dan volgt

$$(7) \quad \text{Lim} \left\{ \frac{f(x)}{\psi'(x)} + \frac{f(x_1)}{\psi'(x_1)} + \dots + \frac{f(x_n)}{\psi'(x_n)} \right\} = \frac{1}{1.2 \dots n} f^n(X).$$

Behalve de onderstellingen die voor de geldigheid der formules (1) en (2) gemaakt moeten worden, moet bij deze laatste formule bovendien nog  $f^n(x)$  voor  $x=X$  continu zijn, daar men anders niet kan besluiten, dat  $f^n(\xi)$  bij convergentie van  $\xi$  tot  $X$ , tot de limiet  $f^n(X)$  convergeert.

Deze formule (7), die dus in het geval, dat  $f^n(x)$  voor  $x=X$  continu is, eene directe algemeene definitie van het  $n^{\text{de}}$  differentiaalquotiënt van eene functie  $f(x)$  geeft, schijnt nog niet in de hier gegeven algemeenheid bewezen te zijn. Wel komt zij voor in het uitstekend werk van Lipschitsch, Differential- und Integralrechnung, p. 204 Form. 20, maar bij het daar voorkomende bewijs moet men onderstellen, dat  $x, x_1, \dots, x_n$  bij hunne convergentie tot de limiet  $X$ , behalve dat zij steeds ongelijk blijven, nog aan andere condities moeten voldoen, die hier overbodig blijken. Zie t. a. p. p. 203, regel 6 v. o. En verder is daar het bestaan van een eindig en continu  $n+1^{\text{ste}}$  differentiaalquotiënt aangenomen. Ook deze conditie ligt stellig in het geheel niet in den aard der zaak, en nadat Weierstrass continue functies heeft leeren kennen, die niet differentieerbaar zijn, zou niet



gemakkelijker zijn dan functiën op te stellen, voor we geldig is, maar waarbij van geen  $n + 1^{\text{ste}}$  differentiaal kan zijn <sup>1)</sup>

5. De overeenkomst van de formule (1) met h Taylor valt nog meer in het oog, wanneer men het niet voorstelt onder de elegante en symmetriek Lagrange gegeven, maar onder den vorm, dien Newton der Principia bij gelegenheid van zijne behandeling probleem geeft.

De formule (1) neemt dan namelijk deze gedaante

$$(8) \quad \dots \quad f(x) = A_1 + A_2(x - x_1) + A_3(x - x_1)(x - x_2) + A_n(x - x_1)(x - x_2) \dots (x - x_{n-1}) + \frac{(x - x_1)(x - x_2) \dots (x - x_n)}{1 \cdot 2 \cdot 3 \dots n} f^{(n)}(x)$$

Hierin is

$$A_1 = f(x_1), \quad A_2 = \frac{f(x_1)}{x_1 - x_2} + \frac{f(x_2)}{x_2 - x_1}$$

en algemeen

$$(9) \quad \dots \quad \begin{cases} A_p = \frac{f(x_1)}{\varphi'_p(x_1)} + \frac{f(x_2)}{\varphi'_p(x_2)} + \dots + \frac{f(x_p)}{\varphi'_p(x_p)} \\ \varphi_p(z) = (z - x_1)(z - x_2) \dots (z - x_p). \end{cases}$$

Newton geeft niet explicite deze algemeene uitdrukkingen, maar wel de volgende rekenvoorschriften om achtereenvolgende termen te berekenen:

$$A_1 = f(x_1), \quad A_2 = \frac{B_1 - A_1}{x_2 - x_1}, \quad A_3 = \frac{B_2 - A_2}{x_3 - x_1}, \quad A_4 = \frac{B_3 - A_3}{x_4 - x_1}, \dots$$

$$B_1 = f(x_2), \quad B_2 = \frac{C_1 - B_1}{x_3 - x_2}, \quad B_3 = \frac{C_2 - B_2}{x_4 - x_2}, \dots$$

Stelt men deze grootheden, zooals zij achtereenvolgens gevonden worden, aldus te zamen

$$(10) \quad \left( \begin{array}{cccc} A_1 & & & \\ & A_2 & & \\ B_1 & & A_3 & \\ & B_2 & & A_4, \\ C_1 & & B_3 & \\ & C_2 & & \\ D_1 & & & \end{array} \right.$$

dan komt deze berekening geheel overeen met die van de gewone interpolatie in het geval, dat  $x_1, x_2, \dots, x_n$  eenerekenkundigereeks vormen, met deze geringe wijziging, dat de 1<sup>ste</sup>, 2<sup>de</sup>, 3<sup>de</sup>, ... rijen van verschillen hier respectieve door de factoren  $1.(x_2 - x_1)$ ,  $1.2.(x_2 - x_1)$ ,  $1.2.3.(x_2 - x_1)^3 \dots$  gedeeld voorkomen.

Volgens de formule (2) is

$$A_p = \frac{1}{1.2.3 \dots (p-1)} f^{p-1}(\xi_p),$$

waarin  $\xi_p$  eene waarde heeft gelegen tusschen het grootste en het kleinste der getallen  $x_1, x_2, \dots, x_p$ . Laat men dus in de formule (8)  $x_1, x_2, \dots, x_p$  tot eenzelfde limiet convergeeren, dan ontstaat onmiddellijk de formule van Taylor met den restvorm van Lagrange.

## 6. De Newton'sche vorm van het interpolatiepolynomium

$$F(x) = A_1 + A_2(x - x_1) + A_3(x - x_1)(x - x_2) + \dots \\ + A_n(x - x_1)(x - x_2) \dots (x - x_{n-1})$$

heeft boven dien van Lagrange ook nog dit voordeel, dat hij onmiddellijk doet zien welken vorm  $F(x)$  aanneemt, wanneer er onder de grootheden  $x_1, x_2, \dots, x_n$  sommige tot eenzelfde limiet convergeeren of gelijk gesteld worden.



Voldoet eene functie  $G(z)$  aan de condities

$$\begin{array}{llll} G(x) = 0, & G'(x) = 0, & \dots, & G^{\alpha-1}(x) = 0, \\ G(y) = 0, & G'(y) = 0, & \dots, & G^{\beta-1}(y) = 0, \\ G(z) = 0, & G'(z) = 0, & \dots, & G^{\gamma-1}(z) = 0, \\ \dots & \dots & \dots & \dots \end{array}$$

waarvan het aantal

$$\alpha + \beta + \gamma \dots = n$$

bedraagt, dan is

$$G^{n-1}(\xi) = 0,$$

waarin  $\xi$  gelegen is tusschen de grootste en de kleinste der ongelijke waarden  $x, y, z, \dots$

Na hetgeen in art. 2 gezegd is, schijnt het niet noodig, bij het bewijs hiervan lang stil te staan. Men kan eerst het geval, dat het grootste der getallen  $\alpha, \beta, \gamma, \dots$  twee is, beschouwen, en vervolgens voor dit grootste onder die getallen 3, 4, 5, ... aannemen.

8. Zij nu  $H(x)$  het polynomium van den  $k-1^{\text{sten}}$  graad hoogstens dat aan de condities (12) voldoet, en

$$(13) \quad f(x) = H(x) + (x-x_1)^{\alpha_1}(x-x_2)^{\alpha_2} \dots (x-x_n)^{\alpha_n} R$$

dan is,  $x$  verschillend van  $x_1, x_2, \dots, x_n$  ondersteld, de waarde van  $f(x)$  hierdoor volkomen bepaald. Beschouwt men nu verder de functie

$$G(z) = -f(z) + H(z) + (z-x_1)^{\alpha_1}(z-x_2)^{\alpha_2} \dots (z-x_n)^{\alpha_n} R,$$

dan is blijkbaar niet alleen

$$G(x) = 0,$$

maar ook

$$\begin{array}{llll} G(x_1) = 0, & G'(x_1) = 0, & \dots, & G^{\alpha_1-1}(x_1) = 0, \\ G(x_2) = 0, & G'(x_2) = 0, & \dots, & G^{\alpha_2-1}(x_2) = 0, \end{array}$$

en ten slotte

$$(14) \quad \left\{ \begin{array}{l} R = \frac{1}{1 \cdot 2 \cdot 3 \dots k} f^k(\xi), \\ f(x) = H(x) + \frac{(x-x_1)^{\alpha_1} (x-x_2)^{\alpha_2} \dots (x-x_n)^{\alpha_n}}{1 \cdot 2 \cdot 3 \dots k} \end{array} \right.$$

Hierin ligt  $\xi$  tusschen het grootste en het kleinste van  $x, x_1, \dots, x_n$ .

In deze formule liggen zoowel de reeks van Taylor als de formule van Lagrange, door een restterm aangevuld, als speciaal gevallen opgesloten.

In de aangehaalde verhandeling stelt Hermite het verschil  $f(x) - H(x)$  met behulp van bepaalde

9. Het algemeenste resultaat, dat door de in § 8 ontwikkelde methode verkregen kan worden, schijnt

Laten  $f(x)$  en  $H(x)$  dezelfde beteekenis behouden. Laten verder  $f_1(x)$  eene nieuwe functie van  $x$  zijn en  $H_1(x)$  een polynoom van  $x$  van den  $k-1^{\text{ste}}$ n graad hoogstens, die aan  $f_1(x)$  voldoet, wanneer men daarin de functie  $f(x)$  door  $f_1(x)$  vervangt.

$$(15) \quad f(x) = H(x) + R(f_1(x) - H_1(x))$$

Zal de waarde van  $R$  hierdoor op ondubbelzinnig bepaald worden, dan moet  $x$  niet alleen van  $x_1, x_2, \dots, x_n$  verschillen, maar mag niet  $f_1(x) - H_1(x) = 0$  worden.

Dit nu onderstellende, zij

$$G(z) = f(z) - H(z) - R(f_1(z) - H_1(z))$$

dan is niet alleen

$$G(x) = 0,$$

maar ook

$$G(x_1) = 0, \quad G'(x_1) = 0, \quad \dots, \quad G^{(\alpha_1)}(x_1) = 0,$$

worden en derhalve heeft men

$$R = \frac{f^k(\xi)}{f_1^k(\xi)},$$

of wel

$$(16) \quad \dots \quad f(x) = H(x) + (f_1(x) - H_1(x)) \frac{f^k(\xi)}{f_1^k(\xi)}.$$

Deze algemeene formule gaat onmiddellijk in de formule (14) over wanneer men aanneemt

$$f_1(x) = x^k.$$

Dan wordt namelijk

$$f_1^k(x) = 1.2.3 \dots k$$

en zooals dadelijk te zien is

$$f_1(x) - H_1(x) = (x - x_1)^{a_1} (x - x_2)^{a_2} \dots (x - x_n)^{a_n}.$$

## N A S C H R I F T.

Dat er altijd één en niet meer dan één functie  $H(x)$  bestaat, die aan de condities (12) voldoet, en hoogstens van den  $k - 1^{\text{sten}}$  graad is, kan onmiddellijk aldus aangetoond worden.

Zij

$$H(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1},$$

dan heeft men ter bepaling van de  $k$  onbekenden  $a_0, a_1, \dots, a_{k-1}$  de volgende  $k$  lineaire vergelijkingen

$$\begin{aligned} a_0 + x_1 a_1 + x_1^2 a_2 + \dots + x_1^{k-1} a_{k-1} &= f(x_1) \\ 1 a_1 + 2 x_1 a_2 + \dots + (k-1) x_1^{k-2} a_{k-1} &= f'(x_1) \\ 1.2. a_2 + \dots + (k-1)(k-2) x_1^{k-3} a_{k-1} &= f''(x_1) \\ \dots &\dots \\ A \dots (a_1 - 1) a_{a_1-1} + \dots + (k-1)(k-2) \dots (k-a_1+1) x_1^{k-a_1} a_{k-1} &= f^{a_1-1}(x_1) \\ &= f^{a_1-1}(\xi) \end{aligned}$$

Vooreerst is nu op te merken, dat het systeem (A) één oplossing kan toelaten, want waren er bijv. twee, dan zoude men dus twee verschillende functies  $G(x)$  vinden die beide aan de voorwaarden, in (12) uitgedrukt, voldoen van den  $k-1^{\text{ste}}$ n graad hoogstens zijn. Dit nu is uit die vergelijkingen (12) zou volgen, dat het verschil

$$G(x) - H(x)$$

algebraïsch deelbaar is door de uitdrukking van den

$$(x - x_1)^{a_1} (x - x_2)^{a_2} \dots (x - x_n)^{a_n}.$$

In de tweede plaats is het evident, dat aan (A) do

$$a_0 = 0, \quad a_1 = 0, \quad a_2 = 0, \quad \dots, \quad a_{k-1} = 0$$

voldaan wordt zoodra de tweede leden der vergelijkingen gesteld worden, en na het bovenstaande is dit ook duidelijk in dit geval

Uit de theorie der lineaire vergelijkingen volgt nu dat de determinant van het stelsel vergelijkingen (A) niet nul is. Uit die theorie is bekend, dat zoodra deze determinant niet nul is, de vergelijkingen (A), nadat daarin voor de tweede leden de waarde nul genomen is, voldaan kan worden door een set waarden  $a_0, a_1, \dots, a_{k-1}$ , die niet allen gelijk nul zijn, wat in overeenstemming met het boven bewezene.

Uit het niet gelijk nul zijn van den determinant van de vergelijkingen (A), volgt nu onmiddellijk, dat aan die vergelijkingen keurige waarden der tweede leden, steeds door een set waarden  $a_0, a_1, \dots, a_{k-1}$  voldaan kan worden.

Men kan overigens de waarde van dien determinant aangeven.

Wanneer men namelijk in onderstaande bekende

$$\begin{vmatrix} 1 & a_0 & a_1^2 & \dots & a_{k-1}^{k-1} \\ \vdots & \vdots & \vdots & \ddots & \vdots \end{vmatrix}$$

de  $a_1$  eerste der grootheden  $a, b, c, \dots, p, q$  tot de limiet  $x_1$ , de  $a_2$  volgende tot de limiet  $x_2$  enz. laat convergeeren, de horizontale rijen op passende wijze transformeert, waarbij men te deelen heeft door de factoren die ten slotte gelijk nul worden, en voorts bij den grensovergang van de formule (7) gebruik maakt, verkrijgt men de navolgende waarde voor den determinant van het stelsel vergelijkingen (A)

$$\begin{array}{ccccccc} 0!1!2!\dots(a_1-1)!(x_2-x_1)^{a_1a_2}(x_3-x_1)^{a_1a_3}\dots(x_n-x_1)^{a_1a_n} & & & & & & \\ 0!1!2!\dots(a_2-1)!(x_3-x_2)^{a_2a_3}\dots(x_n-x_2)^{a_2a_n} & & & & & & \\ \cdot & \cdot & \cdot & \cdot & \cdot & \cdot & \cdot \\ 0!1!2!\dots(a_n-1)!(x_n-x_{n-1})^{a_{n-1}a_n} & & & & & & \end{array}$$

De geheele bewerking blijkt genoegzaam uit het volgende bijzondere geval

$$k=5, n=2, a_1=3, a_2=2.$$

Hier heeft men

$$\begin{vmatrix} 1 & a & a^2 & a^3 & a^4 \\ 1 & b & b^2 & b^3 & b^4 \\ 1 & c & c^2 & c^3 & c^4 \\ 1 & d & d^2 & d^3 & d^4 \\ 1 & e & e^2 & e^3 & e^4 \end{vmatrix} =$$

$$= \begin{vmatrix} 1 & a & a^2 & a^3 & a^4 \\ t_0 & t_1 & t_2 & t_3 & t_4 \\ u_0 & u_1 & u_2 & u_3 & u_4 \\ 1 & d & d^2 & d^3 & d^4 \\ v_0 & v_1 & v_2 & v_3 & v_4 \end{vmatrix} \times (b-a)(c-a)(c-b)(e-d),$$

waarin

$$t = \frac{a^r}{r!} + \frac{b^r}{r!}$$



Derhalve is

$$\begin{vmatrix} 1 & a & a^2 & a^3 & a^4 \\ t_0 & t_1 & t_2 & t_3 & t_4 \\ u_0 & u_1 & u_2 & u_3 & u_4 \\ 1 & d & d^2 & d^3 & d^4 \\ v_0 & v_1 & v_2 & v_3 & v_4 \end{vmatrix} = (d - a) (d - t_0) (d - t_1) (d - t_2) (d - t_3) (d - t_4) (e - a) (e - t_0) (e - t_1) (e - t_2) (e - t_3) (e - t_4)$$

en voor

$$\lim a = \lim b = \lim c = x_1$$

$$\lim e = \lim d = x_2,$$

volgt nu met behulp van de formule (7)

$$\begin{vmatrix} 1 & x_1 & x_1^2 & x_1^3 & x_1^4 \\ 0 & 1 & 2x_1 & 3x_1^2 & 4x_1^3 \\ 0 & 0 & 2 & 2.3x_1 & 3.4x_1^2 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 \\ 0 & 1 & 2x_2 & 3x_2^2 & 4x_2^3 \end{vmatrix} =$$

## IV.

(Amsterdam, Versl. K. Akad. Wet., 1<sup>re</sup> sect., sér. 2, 17,  
1882, 239—254.)  
(traduction)

---

### A propos de la formule d'interpolation de Lagrange.

1. La formule qu'on désigne ordinairement par ce nom fait connaître la fonction entière et rationnelle de  $x$ , du degré  $(n - 1)$  tout au plus qui pour  $n$  valeurs particulières

$$x = x_1, x = x_2, \dots, x = x_n$$

prend la même valeur qu'une fonction arbitraire  $f(x)$ ; cette fonction rationnelle a la forme suivante

$$\sum_{p=1}^{p=n} \frac{\varphi(x)}{(x - x_p) \varphi'(x_p)} f(x_p),$$

où

$$\varphi(x) = (x - x_1)(x - x_2) \dots (x - x_n),$$

et où  $\varphi'(x)$  désigne, comme d'ordinaire, la dérivée de  $\varphi(x)$ .

Si la fonction  $f(x)$  elle-même est rationnelle et du degré  $(n - 1)$  tout au plus, on a identiquement

$$f(x) = \sum_{p=1}^{p=n} \frac{\varphi(x)}{(x - x_p) \varphi'(x_p)} f(x_p)$$

deux manières différentes. Ces formules contiennent les limites, le reste de la série de Taylor.

De même que de l'intégrale définie qui représente le reste de la série de Taylor on peut immédiatement déduire la formule du reste de Lagrange<sup>1)</sup>, de même aussi du cas de la formule d'interpolation de Lagrange déduire la formule multiple, par lequel Hermite représente le reste, de ce reste. Mais aussi bien que dans le cas de la formule d'intégrale on déduit souvent la formule simplifiée de ce reste du calcul intégral, peut-on désirer la même chose pour le reste dans la formule d'interpolation. Nous déduisons la méthode qui conduit à ce but.

Je remarque que Hermite n'a pas donné la formule du reste que nous obtiendrons ici, quoique cette formule puisse être déduite de la sienne. A cet effet il est nécessaire de déduire des intégrales multiples une propriété élémentaire des fonctions définies simples, ce qui n'offre aucune difficulté.

La formule qu'il s'agit de démontrer peut être

$$(1) \quad \dots f(x) = \sum_{p=1}^{p=n} \frac{\varphi(x)}{(x-x_p)\varphi'(x_p)} f(x_p) + \frac{\varphi(x)}{1 \cdot 2 \cdot \dots \cdot n} \varphi^{(n)}(\xi)$$

où  $\xi$  a une valeur intermédiaire entre le plus grand et le plus petit des nombres  $x, x_1, \dots, x_n$ .

Il faut supposer que la fonction  $f(z)$ , aussi bien que  $\varphi(z)$ , soit finie et continue pour toutes les valeurs de  $z$  comprises entre  $x$  et  $x_n$  et que pour ces mêmes valeurs de  $z$  la fonction ait une dérivée  $f^{(n)}(z)$  finie et déterminée.

La formule (1) prend une forme plus élégante si l'on introduit la fonction  $f^{(n)}(\xi)$ ; on se convainc aisément qu'elle est la suivante

On reconnaît dans cette équation un cas plus général de la formule élémentaire

$$\frac{f(x) - f(x_1)}{x - x_1} = f'(\xi),$$

qui s'en déduit lorsqu'on pose  $n = 1$ .

2. La démonstration de la formule (1) repose sur le lemme suivant : „Lorsque la fonction  $G(z)$  prend la valeur zéro pour les  $n + 1$  valeurs différentes  $z = x, z = x_1, \dots, z = x_n$ , la  $n^{\text{ième}}$  dérivée  $G^{(n)}(z)$  devient nulle pour une valeur  $z = \xi$  intermédiaire entre le plus grand et le plus petit des nombres  $x, x_1, \dots, x_n$ .”

Il faut supposer que les fonctions  $G(z), G'(z), \dots, G^{(n-1)}(z)$  soient finies et continues pour toutes les valeurs de  $z$  intermédiaires entre  $x, x_1, \dots, x_n$ , et que, pour les mêmes valeurs de  $z$ ,  $G^{(n-1)}(z)$  ait une dérivée  $G_n(z)$  finie et déterminée.

Ce théorème est connu pour  $n = 1$ ; il suffit de renvoyer à Dini, *Fondamenti per la teorica delle funzioni di variabili reali*, p. 70.

La preuve de ce théorème, aussi bien que de quelques théorèmes qui s'y rattachent telle qu'elle se trouve dans les livres d'étude les plus employés encore aujourd'hui, p. e. dans Serret, *Cours de calcul différentiel et intégral*, contient une lacune qui n'a été comblée que par quelques recherches de Weierstrass; on peut consulter Dini, p. 43—51. Weierstrass lui-même n'a rien publié à ce qu'il paraît de ces recherches sur les bases de la théorie des fonctions.

Il faut surtout remarquer que dans le cas le plus simple de tous celui où  $n = 1$ , la grandeur  $\xi$  est située entre  $x$  et  $x_1$  et qu'on peut lui donner une valeur qui diffère tant de  $x$  que de  $x_1$ .

La preuve du lemme dans le cas général se déduit immédiatement de ce même lemme reconnu comme vrai dans le cas le plus simple celui où  $n = 1$ . En effet, lorsque  $n = 2$ , et par conséquent

et en appliquant encore une fois le théorème pour

$$G''(\xi) = 0. \quad \xi_1 < \xi < \xi_2$$

On peut continuer ainsi et l'on voit en même cas général la grandeur  $\xi$  peut être supposée diff grand et du plus petit des nombres  $x, x_1, \dots, x_n$ . Le doit imposer à la fonction  $G(z)$  et à ses dérivées, celles et dérivables, se déduisent aisément de celles qui cas où  $n = 1$ .

3. La preuve de la formule (1) peut maintenant la suivante.

Pour simplifier, je désigne par  $F(x)$  le polynôme Lagrange; donc

$$(3) \quad \dots \dots F(x) = \sum_{p=1}^{p=n} \frac{\varphi(x)}{(x-x_p)\varphi'(x_p)} f(x_p).$$

Parmi les valeurs  $x_1, x_2, \dots, x_n$  il n'y en a pas de et comme les fonctions  $F(x)$  et  $f(x)$  prennent les m  $x = x_1, x = x_2, \dots, x = x_n$  et que nous nous proposons la formule générale et simple qui exprime la différence pouvons, sans qu'il en résulte aucun inconvénient valeur de  $x$  ne coïncide pas avec une des valeurs

Ceci posé, soit

$$(4) \quad \dots \dots f(x) = F(x) + (x-x_1)(x-x_2)\dots(x-x_n)R$$

La valeur de  $R$  est complètement déterminée par Figurons-nous pour un instant que les grandeurs constantes, tandis que  $z$  représente une nouvelle variable la fonction

$$(5) \quad \dots \dots G(z) = -f(z) + F(z) + (z-x_1)(z-x_2)\dots(z-x_n)$$

où  $\xi$  a une valeur intermédiaire entre le plus grand et le plus petit des nombres  $x, x_1, \dots, x_n$ . Mais comme  $F(z)$  est en  $z$  du degré  $(n-1)$  tout au plus, cette fonction donne zéro lorsqu'on différencie  $n$  fois d'où l'équation (5). On trouve donc

$$G^{(n)}(z) = -f^{(n)}(z) + 1.2.3 \dots n.R.$$

L'équation (6) donne maintenant

$$R = \frac{1}{1.2.3 \dots n} f^{(n)}(\xi)$$

et en substituant cette valeur dans l'équation (4) on obtient

$$f(x) = F(x) + \frac{(x-x_1)(x-x_2) \dots (x-x_n)}{1.2.3 \dots n} f^{(n)}(\xi);$$

nous avons donc trouvé la démonstration de la formule (1).

4. Lorsque, dans la formule (2) qui maintenant a été démontrée elle-même, on laisse tendre vers une même limite  $X$  tous les nombres  $x, x_1, \dots, x_n$ , toujours différents entre eux, il s'ensuit que

$$(7) \quad \lim \left\{ \frac{f(x)}{\psi'(x)} + \frac{f(x_1)}{\psi'(x_1)} + \dots + \frac{f(x_n)}{\psi'(x_n)} \right\} = \frac{1}{1.2.3 \dots n} f^{(n)}(X).$$

Outre les hypothèses qui doivent être faites pour que les formules (1) et (2) soient valables, il faut encore que dans cette dernière formule  $f^{(n)}(x)$  soit continue pour  $x=X$ , attendu qu'il est impossible autrement de conclure que  $f^{(n)}(\xi)$  tend vers la limite  $f^{(n)}(X)$  lorsque  $\xi$  tend vers  $X$ .

Cette formule (7) qui donne donc dans le cas où la fonction  $f^{(n)}(x)$  est continue pour  $x=X$  une définition directe et générale de la  $n^{\text{ième}}$  dérivée d'une fonction  $f(x)$ , n'a pas encore, paraît-il, été démontrée aussi généralement que nous l'avons fait ici. Elle se trouve, il est vrai, dans l'excellent ouvrage de Lipschitsch, *Differential und Integralrechnung*, p. 204, Form. 20, mais d'après la démonstration

exigée par la nature des choses, et après que l'on connaît des fonctions continues qui n'ont pas de dérivées, il serait plus facile que de trouver des fonctions pour lesquelles la formule (7) est valable, sans qu'il puisse être question de la  $n + 1^{\text{ième}}$  de ces fonctions. <sup>1)</sup>

5. L'analogie entre la formule (1) et le théorème plus évidente encore lorsqu'on ne donne pas au polynôme la forme élégante et symétrique que lui donne Lagrange, qui se trouve chez Newton dans le troisième Livre, à l'occasion de la discussion du problème des comètes. La formule (1) prend alors la forme

$$(8) \quad \dots \quad f(x) = A_1 + A_2(x - x_1) + A_3(x - x_1)(x - x_2) + A_4(x - x_1)(x - x_2) \dots (x - x_{n-1}) + \frac{(x - x_1)(x - x_2) \dots (x - x_n)}{1 \cdot 2 \cdot 3 \dots n} f^{(n)}(x)$$

Dans cette équation on a

$$A_1 = f(x_1), \quad A_2 = \frac{f(x_2) - f(x_1)}{x_2 - x_1} + \frac{f(x_2)}{x_2 - x_1}$$

et généralement

$$(9) \quad \dots \quad \begin{cases} A_p = \frac{f(x_1)}{\varphi'_p(x_1)} + \frac{f(x_2)}{\varphi'_p(x_2)} + \dots + \frac{f(x_p)}{\varphi'_p(x_p)} \\ \varphi_p(z) = (z - x_1)(z - x_2) \dots (z - x_p) \end{cases}$$

Newton ne donne pas explicitement cette formule, mais il fait connaître les procédés nécessaires pour la trouver. On trouve ainsi successivement  $A_1, A_2, \dots$  etc. Ce sont les suivants

$$A_1 = f(x_1), \quad A_2 = \frac{B_1 - A_1}{x_2 - x_1}, \quad A_3 = \frac{B_2 - A_2}{x_3 - x_1}, \quad A_4 = \frac{B_3 - A_3}{x_4 - x_1}, \quad \dots$$

Si l'on fait le tableau suivant de ces grandeurs dans l'ordre où on les trouve

$$(10) \quad \begin{array}{cccc} & A_1 & & \\ & & A_2 & \\ & B_1 & & A_3 \\ & & B_2 & & A_4, \\ & C_1 & & B_3 \\ & & C_2 & \\ & D_1 & & \end{array}$$

ce calcul s'accorde entièrement avec celui de l'interpolation ordinaire dans le cas où  $x_1, x_2, \dots, x_n$  forment une progression arithmétique avec cette légère différence que la première, la deuxième, la troisième ... série des différences sont ici divisées respectivement par les facteurs  $1 \cdot (x_2 - x_1)$ ,  $1 \cdot 2 \cdot (x_2 - x_1)^2$ ,  $1 \cdot 2 \cdot 3 \cdot (x_2 - x_1)^3 \dots$  etc.

On a d'après la formule (2)

$$A_p = \frac{1}{1 \cdot 2 \cdot 3 \dots (p-1)} f^{(p-1)}(\xi_p),$$

où  $\xi_p$  a une valeur intermédiaire entre le plus grand et le plus petit des nombres  $x_1, x_2, \dots, x_p$ . Si dans la formule (8) on laisse tendre  $x_1, x_2, \dots, x_n$  vers une même limite, on obtient donc immédiatement la formule de Taylor avec la formule du reste de Lagrange.

## 6. La forme newtonienne du polynôme d'interpolation

$$F(x) = A_1 + A_2(x - x_1) + A_3(x - x_1)(x - x_2) + \dots \\ + A_n(x - x_1)(x - x_2) \dots (x - x_{n-1})$$

et encore sur celle de Lagrange l'avantage de faire voir immédiatement quelle est la forme que prend  $F(x)$  lorsque plusieurs des grandeurs  $x_1, x_2, \dots, x_n$  tendent vers une même limite ou sont prises égales entre elles.





Lorsqu'une fonction  $G(z)$  satisfait aux conditions

$$\begin{aligned} G(x) &= 0, & G'(x) &= 0, & \dots, & G^{(\alpha-1)}(x) &= 0, \\ G(y) &= 0, & G'(y) &= 0, & \dots, & G^{(\beta-1)}(y) &= 0, \\ G(z) &= 0, & G'(z) &= 0, & \dots, & G^{(\gamma-1)}(z) &= 0, \\ & \dots & & & & & \dots \end{aligned}$$

dont le nombre est

$$\alpha + \beta + \gamma \dots = n,$$

on a

$$G^{(n-1)}(\xi) = 0,$$

où  $\xi$  est une grandeur inférieure à la plus grande et supérieure à la plus petite des grandeurs différentes  $x, y, z, \dots$

Après ce qui a été dit au n° 2, il paraît superflu de s'arrêter longtemps à la démonstration de ce théorème. On peut considérer d'abord le cas où le plus grand des nombres  $\alpha, \beta, \gamma, \dots$  est égal à 2, et prendre ensuite 3, 4, 5, ... pour le plus grand de ces nombres.

8. Soit maintenant  $H(x)$  le polynôme du degré  $k-1$  tout au plus qui satisfait aux conditions (12) et soit

$$(13) \quad f(x) = H(x) + (x-x_1)^{\alpha_1}(x-x_2)^{\alpha_2} \dots (x-x_n)^{\alpha_n} R.$$

Alors, si l'on suppose la grandeur  $x$  différente de  $x_1, x_2, \dots, x_n$  la constante  $R$  est complètement déterminée par cette équation. Si l'on considère ensuite la fonction

$$G(z) = -f(z) + H(z) + (z-x_1)^{\alpha_1}(z-x_2)^{\alpha_2} \dots (z-x_n)^{\alpha_n} R$$

il est évident qu'on n'a pas seulement

$$G(x) = 0,$$

mais aussi

$$G(x_1) = 0, \quad G'(x_1) = 0, \quad \dots, \quad G^{(\alpha_1-1)}(x_1) = 0,$$

$$G(x_n) = 0, \quad G'(x_n) = 0, \quad \dots, \quad G^{(\alpha_n-1)}(x_n) = 0.$$



et par conséquent

$$R = \frac{f^{(k)}(\xi)}{f_1^{(k)}(\xi)},$$

ou bien

$$(16) \quad \dots \quad f(x) = H(x) + (f_1(x) - H_1(x)) \frac{f^{(k)}(\xi)}{f_1^{(k)}(\xi)}.$$

Cette formule générale se transforme immédiatement dans la formule (14) lorsqu'on prend

$$f_1(x) = x^k.$$

En effet, on a alors

$$f_1^{(k)}(x) = 1.2.3 \dots k$$

et, comme on peut le voir immédiatement,

$$f_1(x) - H_1(x) = (x - x_1)^{\alpha_1} (x - x_2)^{\alpha_2} \dots (x - x_n)^{\alpha_n}.$$

## POSTSCRIPTUM.

On peut démontrer immédiatement de la façon suivante qu'il existe toujours une et une seule fonction  $H(x)$  qui satisfait aux conditions (12) et qui est en  $x$  du degré  $k - 1$  tout au plus.

Soit

$$H(x) = a_0 + a_1 x + a_2 x^2 + \dots + a_{k-1} x^{k-1}.$$

Pour déterminer les  $k$  grandeurs inconnues  $a_0, a_1, \dots, a_{k-1}$  on a alors les  $k$  équations linéaires suivantes

$$(A) \quad \left\{ \begin{array}{l} a_0 + x_1 a_1 + x_1^2 a_2 + \dots + x_1^{k-1} a_{k-1} = f(x_1) \\ 1 a_1 + 2 x_1 a_2 + \dots + (k-1) x_1^{k-2} a_{k-1} = f'(x_1) \\ 1.2 a_2 + \dots + (k-1)(k-2) x_1^{k-3} a_{k-1} = f''(x_1) \\ \dots \\ (a_1 - 1)! a_{a_1-1} + \dots + (k-1)(k-2) \dots (k-a_1+1) x_1^{k-a_1} a_{k-1} = f^{(a_1-1)}(x_1) \end{array} \right.$$

On peut remarquer d'abord que le système (A) admet une seule solution, car s'il pouvait y avoir plusieurs solutions, il y aurait deux fonctions différentes  $G(x)$  et  $H(x)$  satisfaisant l'autre aux conditions (12) et qui seraient l'une et l'autre de degré  $k-1$  tout au plus. Or, cela est impossible, car il résulterait que la différence

$$G(x) - H(x)$$

est algébriquement divisible par l'expression du déterminant

$$(x - x_1)^{a_1} (x - x_2)^{a_2} \dots (x - x_n)^{a_n}$$

Il est évident en second lieu que les valeurs

$$a_0 = 0, \quad a_1 = 0, \quad a_2 = 0, \quad \dots, \quad a_{k-1} = 0$$

satisfont aux équations (A), aussitôt que les seconds membres sont égaux à zéro; et d'après ce qui précède, c'est la seule solution en ce cas.

La théorie des équations linéaires nous conduit à cette conclusion, que le déterminant du système est nul. En effet, d'après cette théorie on peut dire que si le déterminant est nul, satisfaire aux équations (A), revient à satisfaire partout les seconds membres par zéro, par une fonction de degré  $k-1$ , qui ne sont pas toutes nulles. C'est à ce que nous avons démontré plus haut.

Et de ce que le déterminant du système d'équations est nul, il résulte immédiatement qu'on peut toujours trouver des valeurs arbitraires, satisfaire à ces équations par un seul système de valeurs  $a_0, a_1, \dots, a_{k-1}$ .

D'ailleurs on peut aisément indiquer la valeur de ces coefficients.

A cet effet on peut partir de la formule connue

où les  $a_1$  premières des grandeurs  $a, b, c, \dots, p, q$  tendront à la fin vers la limite  $x_1$ , les  $a_2$  grandeurs qui suivent vers la limite  $x_2$ , etc. Il faut transformer convenablement les lignes de ce déterminant, en les divisant par les facteurs qui s'annulent à la fin et en appliquant à la limite la formule (7). On obtient ainsi pour le déterminant du système d'équations (A) la valeur suivante

$$\begin{array}{l} 0!1!2!\dots(\alpha_1-1)!(x_2-x_1)^{\alpha_1\alpha_2}(x_3-x_1)^{\alpha_1\alpha_3}\dots(x_n-x_1)^{\alpha_1\alpha_n}\\ 0!1!2!\dots(\alpha_2-1)!(x_3-x_2)^{\alpha_2\alpha_3}\dots(x_n-x_2)^{\alpha_2\alpha_n}\\ \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \\ 0!1!2!\dots(\alpha_n-1)!(x_n-x_{n-1})^{\alpha_{n-1}\alpha_n}. \end{array}$$

La suite des opérations est suffisamment évidente d'après la considération d'un cas particulier, celui où

$$k=5, \quad n=2, \quad a_1=3, \quad a_2=2.$$

Ici on trouve

$$= \begin{vmatrix} 1 & a & a^2 & a^3 & a^4 \\ t_0 & t_1 & t_2 & t_3 & t_4 \\ u_0 & u_1 & u_2 & u_3 & u_4 \\ 1 & d & d^2 & d^3 & d^4 \\ v_0 & v_1 & v_2 & v_3 & v_4 \end{vmatrix} \times (b-a)(c-a)(c-b)(e-d),$$

où

Par conséquent on a

$$\begin{vmatrix} 1 & a & a^2 & a^3 & a^4 \\ t_0 & t_1 & t_2 & t_3 & t_4 \\ u_0 & u_1 & u_2 & u_3 & u_4 \\ 1 & d & d^2 & d^3 & d^4 \\ v_0 & v_1 & v_2 & v_3 & v_4 \end{vmatrix} = \begin{matrix} (d-a)(d-b) \\ (e-a)(e-b) \end{matrix}$$

et en prenant

$$\lim a = \lim b = \lim c = x_1,$$

$$\lim e = \lim d = x_2,$$

on trouve maintenant à l'aide de la formule (7)

$$\begin{vmatrix} 1 & x_1 & x_1^2 & x_1^3 & x_1^4 \\ 0 & 1 & 2x_1 & 3x_1^2 & 4x_1^3 \\ 0 & 0 & 2 & 2.3x_1 & 3.4x_1^2 \\ 1 & x_2 & x_2^2 & x_2^3 & x_2^4 \\ 0 & 1 & 2x_2 & 3x_2^2 & 4x_2^3 \end{vmatrix} = 2(x_1 - x_2)^5$$

## V.

(Amsterdam, Nieuw Arch. Wisk., IX, 1882, 106—

---

### Eenige opmerkingen omtrent de differentiaalquotient van eene functie van één veranderlijke.

Is eene functie  $f(x)$  voor alle waarden van  $x$ ,  $a \leq x \leq b$ , gegeven, voor al deze waarden van  $x$  differentieerbaar, dan is

$$(A) \quad \dots \dots \dots \frac{f(b) - f(a)}{b - a} = f'(\xi).$$

$$(a < \xi < b)$$

Hieruit volgt, wanneer  $a$  en  $b$  tot een limiet  $X$  convergeren,  $f'(x)$  continu is voor  $x = X$ ,

$$(B) \quad \dots \dots \dots \lim \frac{f(b) - f(a)}{b - a} = f'(X).$$

Dat voor de geldigheid van deze formule (B) de voorwaarde, dat  $f'(x)$  voor  $x = X$  continu is, noodzakelijk is, blijkt uit het volgende voorbeeld. Zij  $f(0) = 0$  en voor  $x \geq 0$

$$f(x) = x^2 \cos \left( \frac{\pi}{x^2} \right).$$

De functie  $f(x)$  is dan continu en differentieerbaar voor alle waarden van  $x$ ; in het bijzonder is  $f'(0) = 0$ . Daarentegen is  $f'(x)$  niet overal continu, en namelijk discontinu voor  $x = 0$ .



Neemt nu  $n$  in 't oneindige toe, dan convergeert  
en toch convergeert

$$\frac{f(p_n) - f(p_{n+1})}{p_n - p_{n+1}}$$

niet tot de waarde  $f'(0) = 0$ .

Men overtuigt zich zelfs gemakkelijk er van dat, indien een positief getal  $h$  ook gegeven is, men steeds twee punten  $p$  en  $q$ , beide kleiner dan  $h$ , kan bepalen, zoodanig dat

$$\frac{f(p) - f(q)}{p - q}$$

eene willekeurig voorgeschreven waarde aanneemt. Het spreekt vanzelf, dat sprake zijn van de convergentie van deze uitdrukking tot de bepaalde limiet.

Wordt dus omtrent de wijze, waarop  $a$  en  $b$  naar  $X$  convergeeren, niets anders bepaald, dan is het voldoende, dat  $f'(x)$  voor  $x = X$  continu is, noodzakelijk is de afgeleide digheid van (B).

Zoodra echter vastgesteld wordt, dat  $a$  en  $b$  naar  $X$  convergeeren, dat  $X$  steeds tusschen  $a$  en  $b$  minste niet buiten het interval  $a, b$  valt, dan is het voldoende, reeds, zoodra slechts  $f(x)$  voor  $x = X$  een eindige afgeleide  $f'(X)$  heeft. Het is dan zelfs niet noodig, dat  $f(x)$  voor  $x = X$  van  $x$  differentieerbaar is.

Om dit te bewijzen heeft men niet van (A) gebruik te maken. Volgens de formule de differentieerbaarheid van  $f(x)$  voor  $x = X$  kan men onderstelt, maar men kan uitgaan van de identiteit

$$\frac{f(b) - f(a)}{b - a} = \frac{f(b) - f(X) + f(X) - f(a)}{b - X + X - a}$$

Ligt nu  $X$  in het interval  $a, b$ , dan hebben

welke beide waarden volgens de onderstelling, dat  $f(x)$  voor  $x = X$  een eindig differentiaalquotiënt heeft, tot  $f(X)$  convergeeren; derhalve ook  $\frac{f(b) - f(a)}{b - a}$ . Het is duidelijk, dat  $a$  of  $b$  ook gelijk  $X$  mogen worden.

Als een voorbeeld kan de functie  $f(x)$  dienen, bepaald door  $f(0) = 0$  en voor  $x \geq 0$ , door  $f(x) = \pm x^2$  waarin het bovenste of onderste teken te nemen is, naargelang  $x$  meetbaar of onmeetbaar is. Deze functie heeft alleen voor  $x = 0$  een differentiaalquotiënt, waarvan de waarde door de formule (B) gevonden kan worden, zoolang nul niet buiten het interval  $a, b$  valt.

De formule (A) vormt een bijzonder geval van de volgende meer algemeene, waarvan ik het bewijs elders<sup>1)</sup> gegeven heb.

Zij

$$r(z) = (z - x_1)(z - x_2) \dots (z - x_{n+1}),$$

$$(x_1 < x_2 < x_3 \dots < x_n < x_{n+1})$$

laten  $f(x), f'(x), f''(x), \dots, f^{(n-1)}(x)$  continu zijn voor alle waarden van  $x$ ,  $x_1 \leq x \leq x_{n+1}$ , terwijl voor deze zelfde waarden  $f^{(n-1)}(x)$  een eindig differentiaalquotiënt  $f^{(n)}(x)$  heeft; dan is

$$(AA) \quad \dots \quad \sum_{p=1}^{p=n+1} \frac{f(x_p)}{r'(x_p)} = \frac{1}{1 \cdot 2 \cdot 3 \dots n} f^{(n)}(\xi).$$

$$(x_1 < \xi < x_{n+1})$$

Hieruit volgt, wanneer  $x_1, x_2, \dots, x_{n+1}$  tot eene gemeenschappelijke limiet  $X$  convergeeren, en bovendien nog  $f^{(n)}(x)$  voor  $x = X$  continu is,

$$(BB) \quad \dots \quad \sum_{p=1}^{p=n+1} \frac{f(x_p)}{r'(x_p)} = \frac{1}{1 \cdot 2 \cdot 3 \dots n} f^{(n)}(X).$$

Wij zagen reeds boven in het bijzonder geval  $n=1$ , dat in het algemeen de voorwaarde omtrent de continuïteit van  $f^{(n)}(x)$  nood

vang; en wel is het dan voldoende, dat  $f^{(n-1)}(x)$  voor de waarde  $x=X$  een eindig differentiaalquotiënt  $f^{(n)}(X)$  heeft. Het is zelfs niet noodig, dat  $f^{(n-1)}(x)$  voor andere waarden van  $x$  differentieerbaar is, laat staan dan een continu differentiaalquotiënt zooals boven ondersteld moest worden.

Het bewijs hiervan, dat het eigenlijke doel van de onderstelling uitmaakt, kan aldus gevoerd worden.

Zij

$$\varphi(x) = f(x) - \frac{k}{1 \cdot 2 \cdot 3 \dots n} x^n,$$

dan zijn ook

$$\varphi(x), \varphi'(x), \dots, \varphi^{(n-1)}(x),$$

volkomen bepaald, en  $\varphi^{(n-1)}(x)$  heeft voor  $x=X$  een eindig differentiaalquotiënt  $\varphi^{(n)}(X)=0$ . In het voorbijgaan zij op de onderstelling, voor  $x=X$  is  $f^{(n-1)}(x)$  differentieerbaar,  $f^{(n-1)}(x)$  is voor  $x=X$  continu.

Ik stel nu

$$\begin{aligned} p(z) &= (z-x_1)(z-x_2)\dots(z-x_n), \\ q(z) &= (z-x_2)(z-x_3)\dots(z-x_{n+1}), \end{aligned}$$

dan is volgens (AA), wanneer men in deze formules  $x$  vervangt,

$$\sum_{p=1}^{p=n} \frac{\varphi(x_p)}{p'(x_p)} = \frac{1}{1 \cdot 2 \cdot 3 \dots (n-1)} \varphi^{(n-1)}(\xi),$$

$$(x_1 < \xi < x_n),$$

$$\sum_{p=2}^{p=n+1} \frac{\varphi(x_p)}{q'(x_p)} = \frac{1}{1 \cdot 2 \cdot 3 \dots (n-1)} \varphi^{(n-1)}(\eta),$$

$$(x_2 < \eta < x_{n+1})$$

en wel vereischen deze formules geenerlei onderstelling van differentieerbaarheid van  $\varphi^{(n-1)}(x)$ .

$$\left( \frac{\eta - X}{x_{n+1} - x_1} \right) \cdot \frac{\varphi^{(n-1)}(\eta) - \varphi^{(n-1)}(X)}{\eta - X} + \left( \frac{X - \xi}{x_{n+1} - x_1} \right) \cdot \frac{\varphi^{(n-1)}(X) - \varphi^{(n-1)}(\xi)}{X - \xi}.$$

Daar  $\xi$  en  $\eta$  binnen het interval  $x_1, x_{n+1}$  liggen, en  $X$  ten minste niet buiten dit interval ligt, zoo zijn

$$\frac{\eta - X}{x_{n+1} - x_1} \text{ en } \frac{X - \xi}{x_{n+1} - x_1},$$

volstrekt genomen, kleiner dan één. Verder volgt uit de onderstelling dat  $\varphi^{(n-1)}(x)$  voor  $x = X$  een eindig differentiaalquotiënt  $\varphi^{(n)}(X) =$  heeft, dat

$$\frac{\varphi^{(n-1)}(\eta) - \varphi^{(n-1)}(X)}{\eta - X} \text{ en } \frac{\varphi^{(n-1)}(X) - \varphi^{(n-1)}(\xi)}{X - \xi}$$

tot de limiet nul convergeeren, wanneer  $x_1, x_2, \dots, x_{n+1}$  allen tot hun limiet  $X$  convergeeren. Dus volgt ten slotte

$$\lim \sum_{p=1}^{p=n+1} \frac{\varphi(x_p)}{r'(x_p)} = 0,$$

of, daar

$$\varphi(x) = f(x) - \frac{k}{1.2.3 \dots n} x^n$$

was en men identiek heeft

$$\sum_{p=1}^{p=n+1} \frac{x_p^n}{r'(x_p)} = 1,$$

$$\lim \sum_{p=1}^{p=n+1} \frac{f(x_p)}{r'(x_p)} = \frac{k}{1.2.3 \dots n} = \frac{f^{(n)}(X)}{1.2.3 \dots n},$$

waarmee het bedoelde bewijs geleverd is.

Men kan zeggen, dat deze formule altijd geldt, zoodra slechts  $f^{(n)}(X)$  eene bepaalde beteekenis heeft, want dit vordert reeds vanzelf, dat  $f^{(n-1)}(x)$  in de nabijheid van  $x = X$  overal eene eindige en continue veranderlijke waarde heeft: evenzoo wat  $f^{(n-2)}(x)$ ,  $f^{(n-3)}(x)$ , ... betreft.

bestaat. Dit blijkt, wanneer men bedenkt, dat de waarde van  $f(x)$  voor  $x = X$  de bovenstaande waarde verandert, zoolang geen der waarden  $x_1$  aan  $X$  is.

Ligt  $X$  buiten het interval  $x_1, x_{n+1}$ , dan behoeft

$$\frac{\eta - X}{x_1 - x_{n+1}} \text{ en } \frac{X - \xi}{x_1 - x_{n+1}},$$

geen echte breuken meer te zijn, en deze omstandigheden het bewijs ten einde te voeren. Maar wij zagen reeds in het beeld, dat in dit geval omtrent  $f^{(n-1)}(x)$  verdere omstandigheden zijn, namelijk, dat in het algemeen  $f^{(n)}(x)$  bestendig continu is.

## V.

(Amsterdam, Nieuw Arch. Wisk., IX, 1882, 106—III.)

(translation)

### Quelques remarques à propos des dérivées d'une fonction d'une seule variable.

Lorsqu'une fonction  $f(x)$  est donnée pour toutes les valeurs de  $x$  pour lesquelles  $a \leq x \leq b$ , et qu'elle peut être différenciée pour toutes ces valeurs de  $x$ , on a

$$\text{A) } \dots \dots \dots \frac{f(b) - f(a)}{b - a} = f'(\xi).$$

$$(a < \xi < b)$$

Il s'ensuit que lorsque  $a$  et  $b$  tendent vers une limite  $X$  et que la fonction  $f'(x)$  est continue pour  $x = X$ ,

$$\text{B) } \dots \dots \dots \lim \frac{f(b) - f(a)}{b - a} = f'(X).$$

L'exemple suivant fait voir que la condition, d'après laquelle la fonction  $f'(x)$  est continue pour  $x = X$ , doit nécessairement être remplie pour que la formule (B) soit valable.

Exemple. Soit  $f(x) = 0$ , et pour  $x \geq 0$

$$f(x) = x^2 \cos \left( \frac{\pi}{x^2} \right).$$

La fonction  $f(x)$  est alors continue et peut être différenciée pour

il s'ensuit que

$$\frac{f(p_n) - f(p_{n+1})}{p_n - p_{n+1}} = (-1)^n \left( \sqrt{\frac{n}{n+1}} + \sqrt{\frac{n+1}{n}} \right) (V$$

Lorsque  $n$  tend vers l'infini,  $p_n$  converge vers la dant l'expression

$$\frac{f(p_n) - f(p_{n+1})}{p_n - p_{n+1}}$$

ne tend pas vers la valeur  $f'(0) = 0$ .

On se convainc même aisément de ce que, que un nombre donné  $h$ , on peut toujours trouver deux  $p$  et  $q$ , inférieurs à  $h$ , tels que l'expression

$$\frac{f(p) - f(q)}{p - q}$$

prend une valeur quelconque donnée. Il ne peut d'une convergence de cette expression vers une limite.

Nous avons dit que la condition nommée, d'après  $f'(x)$  est continue pour  $x = X$ , doit nécessairement que la formule (B) soit valable, dans l'hypothèse laquelle  $a$  et  $b$  tendent vers leur limite  $X$  est incon

Mais dès qu'on admet que  $a$  et  $b$  tendent vers leur manière que  $X$  reste constamment entre  $a$  et  $b$ , ou pas en dehors de l'intervalle  $a, b$ , la formule (B)  $f(x)$  a pour  $x = X$  une dérivée finie  $f'(X)$ . Dans ce cas nécessaire que  $f(x)$  possède une dérivée pour d'a

Pour le démontrer il n'est pas nécessaire de par qui suppose que la fonction  $f(x)$  peut être différent valeurs de  $x$  pour lesquelles  $a \leq x \leq b$ , on peut comme suit.

Nous avons

a une valeur intermédiaire entre

$$\frac{f(b) - f(X)}{b - X} \quad \text{et} \quad \frac{f(X) - f(a)}{X - a},$$

deux expressions qui tendent vers  $f'(X)$  dans l'hypothèse que  $f(x)$  pour  $x = X$  une dérivée finie; il en est donc de même pour  $\frac{f(b) - f(a)}{b - a}$ . Il est évident que les grandeurs  $a$  et  $b$  peuvent aussi, l'une ou l'autre devenir égales à  $X$ .

Nous pouvons prendre pour exemple la fonction  $f(x)$ , déterminée par  $f(0) = 0$  et par  $f(x) = \pm x^2$  pour  $x \geq 0$ . Il faut prendre le signe supérieur ou le signe inférieur selon que  $x$  est rationnel ou non. Cette fonction ne possède une dérivée que pour  $x = 0$ , dérivée dont on peut trouver la valeur par la formule (B), tant que zéro ne tombe pas en dehors de l'intervalle  $a, b$ .

La formule (A) constitue un cas particulier de la formule suivante plus générale, dont j'ai donné la démonstration ailleurs.<sup>1)</sup>

Soit

$$r(z) = (z - x_1)(z - x_2) \dots (z - x_{n+1}),$$

$$(x_1 < x_2 < x_3 \dots < x_n < x_{n+1})$$

et supposons les fonctions  $f(x), f'(x), f''(x), \dots, f^{(n-1)}(x)$  continues pour toutes les valeurs de  $x$  pour lesquelles  $x_1 \leq x \leq x_{n+1}$  tandis que  $f^{(n-1)}(x)$  a pour ces mêmes valeurs une dérivée finie  $f^{(n)}(x)$ . Nous avons alors

$$\text{AA)} \quad \dots \quad \sum_{p=1}^{p=n+1} \frac{f(x_p)}{r'(x_p)} = \frac{1}{1.2.3 \dots n} f^{(n)}(\xi).$$

$$(x_1 < \xi < x_{n+1})$$

Il s'ensuit que lorsque  $x_1, x_2, \dots, x_{n+1}$  tendent vers une limite commune  $X$  et que de plus la fonction  $f^{(n)}(x)$  est continue pour  $x = X$



Nous avons déjà vu plus haut dans le cas particulier la condition relative à la continuité de  $f^{(n)}$ .

Mais si l'on suppose qu'en convergeant vers  $X$  les  $x_{n+1}$  sont l'une supérieure l'autre inférieure à  $X$ , on ne tombe pas en dehors de l'intervalle  $x_1, x_n$  et on a une signification bien plus générale: il suffit alors de supposer valable que la fonction  $f^{(n-1)}(x)$  ait pour la valeur  $k$  une dérivée finie  $f^{(n)}(X) = k$ . Il n'est pas même nécessaire qu'elle ait une dérivée pour d'autres valeurs de  $x$ , moi que la fonction ait une dérivée continue, comme nous l'avons vu plus haut.

La preuve de cette affirmation qui constitue le but de cette communication, peut être donnée comme suit.

Soit

$$\varphi(x) = f(x) - \frac{k}{1.2 \dots n} x^n,$$

alors

$$\varphi(x), \varphi'(x), \dots, \varphi^{(n-1)}(x)$$

sont elles aussi complètement déterminées et  $\varphi^{(n)}(x) = k$  pour  $x = X$  une dérivée finie  $\varphi^{(n)}(X) = 0$ . Je remarque que l'hypothèse d'après laquelle  $f^{(n-1)}(x)$  peut être différentiable permet déjà de conclure que la fonction  $f^{(n-1)}(x)$  est continue.

Je pose maintenant

$$p(z) = (z - x_1)(z - x_2) \dots (z - x_n)$$

$$q(z) = (z - x_2)(z - x_3) \dots (z - x_n)$$

On a alors d'après la formule (AA), lorsqu'on y remplace

$$\sum_{p=1}^{p=n} \frac{\varphi(x_p)}{p'(x_p)} = \frac{1}{1.2.3 \dots (n-1)} \varphi^{(n-1)}(x)$$

( $x_1 < \xi < x_n$ )

On trouve maintenant en soustrayant et en divisant par  $x_{n+1} - x_1$

$$\sum_{p=1}^{p=n+1} \frac{\varphi(x_p)}{r'(x_p)} = \frac{1}{1.2.3 \dots (n-1)} \left\{ \frac{\varphi^{(n-1)}(\eta) - \varphi^{(n-1)}(\xi)}{x_{n+1} - x_1} \right\}$$

L'expression entre parenthèses qui figure au second membre peut être remplacée par

$$\left( \frac{\eta - X}{x_{n+1} - x_1} \right) \cdot \frac{\varphi^{(n-1)}(\eta) - \varphi^{(n-1)}(X)}{\eta - X} + \left( \frac{X - \xi}{x_{n+1} - x_1} \right) \cdot \frac{\varphi^{(n-1)}(X) - \varphi^{(n-1)}(\xi)}{X - \xi}$$

Comme les grandeurs  $\xi$  et  $\eta$  sont situées dans l'intervalle  $x_1, x_{n+1}$  et que  $X$  n'est certainement pas en-dehors de cet intervalle, les expressions

$$\frac{\eta - X}{x_{n+1} - x_1} \quad \text{et} \quad \frac{X - \xi}{x_{n+1} - x_1}$$

sont, en valeur absolue, inférieures à l'unité. De plus l'hypothèse d'après laquelle  $\varphi^{(n-1)}(x)$  possède pour  $x=X$  une dérivée finie  $\varphi^{(n)}(X)=0$ , nous permet de conclure que les expressions

$$\frac{\varphi^{(n-1)}(\eta) - \varphi^{(n-1)}(X)}{\eta - X} \quad \text{et} \quad \frac{\varphi^{(n-1)}(X) - \varphi^{(n-1)}(\xi)}{X - \xi}$$

convergent vers la limite zéro, lorsque les grandeurs  $x_1, x_2, \dots, x_{n+1}$  tendent toutes vers leur limite  $X$ . On trouve donc enfin

$$\lim \sum_{p=1}^{p=n+1} \frac{\varphi(x_p)}{r'(x_p)} = 0,$$

mais, comme on a

$$\varphi(x) = f(x) - \frac{k}{1.2.3 \dots n} x^n$$

et, identiquement

$$\sum_{p=1}^{p=n+1} \frac{x_p^n}{r'(x_p)} = 1$$

fonction  $f^{(n-1)}(x)$  a alors partout dans le voisinage de  $x$  une valeur finie et continue, et qu'il en est de même pour  $f^{(n-2)}$ .

Mais on ne peut pas affirmer réciproquement qu'une

$$\lim_{p \rightarrow \infty} \sum_{p=1}^{p=n+1} \frac{f(x_p)}{r'(x_p)}$$

a une valeur finie déterminée, cette valeur est  $\frac{f^{(n)}(X)}{1.2}$ .

Il est fort bien arrivé que même alors  $f^{(n)}(X)$  n'existe pas. On peut remarquer que lorsqu'on substitue  $x = X$  dans  $f^{(n)}$  on trouve ci-dessus garde la même valeur, tant qu'aucun des points  $x_1, x_2, \dots, x_{n+1}$  n'est égale à  $X$ .

Lorsque  $X$  est en-dehors de l'intervalle  $x_1, x_{n+1}$

$$\frac{\eta - X}{x_1 - x_{n+1}} \text{ et } \frac{X - \xi}{x_1 - x_{n+1}}$$

ne sont pas nécessairement des fractions inférieures à 1. Dans cette circonstance, lorsqu'elle se présente, nous employons la démonstration à sa fin. Mais nous avons déjà vu que dans ce cas de nouvelles hypothèses relatives à  $f^{(n)}$  sont nécessaires: il faut supposer alors en général que cette fonction est continue pour  $x = X$ .

## VI.

(Amsterdam, Nieuw Arch. Wisk., IX, 1882, 98—106.)

---

### Over eenige theorema's omtrent oneindige reeksen.

1. In het 89<sup>ste</sup> deel van het Journal für die reine und angewandte Mathematik, p. 242—244, geeft de heer G. Frobenius in een kort opstel, Über die Leibnizsche Reihe, een theorema, dat aldaar ten slotte onder den volgenden vorm uitgesproken wordt.

„Ist  $s_n$  eine von  $n$  abhängige Grösse, und nähert sich

$$\frac{s_0 + s_1 + \dots + s_{n-1}}{n}$$

bei wachsendem  $n$  einer bestimmten endlichen Grenze, so nähert sich

$$(1 - x)(s_0 + s_1 x + s_2 x^2 + s_3 x^3 + \dots)$$

falls  $x$  beständig zunehmend gegen Eins convergirt, derselben Grenze.

Dit theorema vertoont eenige analogie met een ander, dat mij sedert lang bekend was en waarvan de waarheid, naar het mij toeschijnt, mij eenig nadenken van zelf duidelijk is; reden, waarom ik indertijd het volledig uitwerken van een streng bewijs naliet. Het stukje van den heer Frobenius geeft mij nu echter aanleiding, het hierop betrekking hebbende eenigzins te ontwikkelen, en er eenige opmerkingen aan toe te voegen; waarbij het blijkt, dat men algemeener kan

wanneer  $x$  steeds toenemend tot de limiet 1 convergeert als

$$\frac{s_0 + s_1 + \dots + s_{n-1}}{n} \text{ voor } n = \infty$$

De vorm van het bewijs van Frobenius schied ik wenschen over te laten, en ik heb daarom niet geheel te volgen.

2. Het boven bedoelde theorema bestaat in dat  $a_0, a_1, a_2, \dots$  alle positief, of ten minste niet negatief, de reeks

$$\psi(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

voor alle waarden  $0 < x < 1$ , maar divergeert dan volgt hieruit van zelf, dat  $\psi(x)$  boven  $1$  convergeert, wanneer  $x$ , steeds toenemend, tot 1 convergeert.

$$s_0, s_1, s_2, \dots$$

eene onbepaald voortlopende rij getallen, die tot  $1$  vergeeren<sup>1)</sup>, dan is het duidelijk, dat ook de reeks

$$f(x) = a_0 s_0 + a_1 s_1 x + a_2 s_2 x^2 + \dots$$

voor alle waarden  $0 < x < 1$  convergeert.

In deze onderstellingen nu bestaat de te bewijzen hierin, dat

$$\frac{f(x)}{\psi(x)}$$

tot de limiet  $M$  convergeert, terwijl  $x$  steeds tot  $1$  nadert.

De omtrent de rij getallen

$$s_0, s_1, s_2, \dots$$

gemaakte onderstelling heeft dezen zin: hoe kleiner  $\epsilon$  ook gegeven is, het is altijd mogelijk, een  $x$  te vinden, zoodat

$$1) \quad \dots \quad s_{n+k} = M + \varepsilon_k, \\ (k = 0, 1, 2, 3, \dots)$$

de volstrekte waarden van

$$\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$$

alle kleiner dan  $\varepsilon$  zijn.

Zij nu

$$2) \quad \dots \quad \begin{cases} P = a_0 s_0 + a_1 s_1 x + a_2 s_2 x^2 + \dots + a_{n-1} s_{n-1} x^{n-1}, \\ Q = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1}, \end{cases}$$

dan volgt, met behulp van (1),

$$f(x) = P + a_n x^n (M + \varepsilon_0) + a_{n+1} x^{n+1} (M + \varepsilon_1) + a_{n+2} x^{n+2} (M + \varepsilon_2) + \dots$$

zoodat  $f(x)$  eene waarde heeft, gelegen tusschen

$$P + (M + \varepsilon) (\psi(x) - Q)$$

en

$$P + (M - \varepsilon) (\psi(x) - Q),$$

waaruit volgt, dat  $f(x) : \psi(x)$  ligt tusschen

$$M + \varepsilon + \frac{P - Q(M + \varepsilon)}{\psi(x)}$$

en

$$M - \varepsilon + \frac{P - Q(M - \varepsilon)}{\psi(x)}.$$

Wanneer nu  $x$  tot 1 convergeert, convergeeren  $P$  en  $Q$  tot zeker eindige limieten, terwijl volgens de onderstelling,  $\psi(x)$  boven alle grenzen toeneemt. Men zal dus  $x$  kleiner dan 1, maar zoo dicht bij 1 kunnen nemen, dat de volstrekte waarden van

$$\frac{P - Q(M + \varepsilon)}{\psi(x)} \quad \text{en} \quad \frac{P - Q(M - \varepsilon)}{\psi(x)}$$

kleiner zijn dan een geheel willekeurig gegeven positief getal  $\delta$ , en kleiner dan  $\delta$  blijven, wanneer  $x$  nog dichter bij 1 genomen wordt.

twee positieve getallen  $\beta = \delta + \varepsilon$ . Bij de waarde evenals boven; namelijk men neme  $n$  zoo groot gesteld zijnde,  $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$  volstrekt genomen alle Nadat dus  $n$  en daarmee ook  $P$  en  $Q$  bekend zijn door de voorwaarde, dat de volstrekte waarden v

$$\frac{P - Q(M + \varepsilon)}{\psi(x)} \text{ en } \frac{P - Q(M - \varepsilon)}{\psi(x)}$$

voor alle waarden  $1 - \alpha \leq x < 1$ , kleiner dan  $\delta$  bli

Volgens het bovenstaande ligt dan, voor deze

$$\frac{f(x)}{\psi(x)}$$

tusschen  $M + \varepsilon + \delta$  en  $M - \varepsilon - \delta$ , d. w. z. tusschen

Het is duidelijk, dat de onderstelling dat  $\psi(x)$  e gerangschikt volgens de geheele opklimmende de bovenstaande afleiding eigenlijk geene ro uitkomst gemakkelijk in een algemeener vorm ui den. Hierbij moet echter opgemerkt worden, da van de redeneering hierin bestaat, dat  $s_n, s_{n+1}$ , veranderlijke  $x$  afhangen, zoodat de bepaling va kelijk is van de bijzondere waarden, die men la toe te schrijven.

3. Als een voorbeeld van de bruikbaarheid va rema kan de hypergeometrische reeks dienen

$$F(a, \beta, \gamma, x) = 1 + \frac{a \cdot \beta}{1 \cdot \gamma} x + \frac{a(a+1) \beta(\beta+1)}{1 \cdot 2 \cdot \gamma(\gamma+1)} x^2 + \dots$$

Hierbij komen dus alleen die gevallen in aan reeks voor  $x=1$  divergeert.

2) De termen nemen boven alle grenzen toe, wanneer positief is.

3) De termen convergeeren tot eene eindige, van 0 limiet, wanneer  $\alpha + \beta - \gamma - 1 = 0$ .

4) De termen convergeeren tot nul, wanneer  $\alpha + \beta - \gamma$  negatief is.

5) De reeks convergeert voor  $x=1$ , wanneer  $\alpha + \beta - \gamma > 0$  is.

Volgens 3) convergeert de uitdrukking

$$\frac{\alpha(\alpha+1)\dots(\alpha+n-1)\beta(\beta+1)\dots(\beta+n-1)}{1.2.3\dots n\dots\gamma(\gamma+1)\dots(\gamma+n-1)}$$

waarin  $\alpha + \beta - \gamma - 1 = 0$ , voor  $n = \infty$ , tot eene eindige limiet gelijk is aan

$$\frac{\Pi(\gamma-1)}{\Pi(\alpha-1)\Pi(\beta-1)}.$$

Iets algemeener vindt men voor  $\alpha + \beta - \gamma - u = 0$

$$(3) \cdot \lim_{n=\infty} \frac{\alpha(\alpha+1)\dots(\alpha+n-1)\beta(\beta+1)\dots(\beta+n-1)}{u(u+1)\dots(u+n-1)\gamma(\gamma+1)\dots(\gamma+n-1)} = \frac{\Pi(u)}{\Pi(\alpha)}$$

en wel volgt dit onmiddellijk uit de definitie van  $\Pi(z)$ :

$$\Pi(z) = \lim_{n=\infty} \frac{1.2.3\dots n}{(z+1)(z+2)\dots(z+n)} n^z.$$

Daar alleen de gevallen, waarin de reeks voor  $x=1$  divergeert, beschouwd worden, zoo ziet men uit 5), dat  $\alpha + \beta - \gamma > 0$  moet worden. De gevallen  $\alpha + \beta - \gamma > 0$  en  $\alpha + \beta - \gamma < 0$  afzonderlijk behandeld worden.

I.  $\alpha + \beta - \gamma > 0$ .

Dan is dus  $u = \alpha + \beta - \gamma$  positief; neemt men nu, volgens de meene theorema

$$s_0 = 1, \quad s_n = \frac{\alpha(\alpha+1)\dots(\alpha+n-1)\beta(\beta+1)\dots(\beta+n-1)}{u(u+1)\dots(u+n-1)\gamma(\gamma+1)\dots(\gamma+n-1)},$$

$$a_0 = 1, \quad a_n = \frac{u(u+1)\dots(u+n-1)}{1.2.3\dots n};$$



$$\begin{aligned}\psi(x) &= a_0 + a_1 x + a_2 x^2 + \dots = (1-x)^{-\gamma} \\ f(x) &= a_0 s_0 + a_1 s_1 x + a_2 s_2 x^2 \dots = F(\alpha, \beta, \gamma, x)\end{aligned}$$

en volgens (3)

$$\lim_{n \rightarrow \infty} s_n = M = \frac{\Pi(u-1) \Pi(\gamma-1)}{\Pi(a-1) \Pi(\beta-1)}$$

zoodat men onmiddellijk verkrijgt

$$(4) \quad \lim_{x \rightarrow 1} (1-x)^{\alpha+\beta-\gamma} F(\alpha, \beta, \gamma, x) = \frac{\Pi(\alpha+\beta-\gamma)}{\Pi(\alpha-1) \Pi(\beta-1)}$$

$$\text{II.} \quad \alpha + \beta - \gamma = 0.$$

Neemt men, om dit geval te behandelen

$$s_0 = \frac{1}{\alpha}, \quad s_n = \frac{(a+1)(a+2)\dots(a+n)\beta(\beta+1)\dots}{1 \cdot 2 \cdot 3 \dots n \cdot \gamma(\gamma+1)\dots(\gamma+n)}$$

$$a_0 = \alpha, \quad a_n = \frac{\alpha}{n+1};$$

dan is

$$\psi(x) = a + \frac{1}{2} a x + \frac{1}{3} a x^2 + \dots = \frac{a}{x} \log \frac{1}{1-x}$$

$$\lim_{n \rightarrow \infty} s_n = \frac{\Pi(\gamma-1)}{\Pi(\alpha) \Pi(\beta-1)} = \frac{\Pi(\alpha+\beta-\gamma)}{\alpha \Pi(\alpha-1) \Pi(\beta-1)}$$

en na eene kleine herleiding

$$(5) \quad \dots \lim_{x \rightarrow 1} \frac{F(\alpha, \beta, \alpha+\beta, x)}{\log \left( \frac{1}{1-x} \right)} = \frac{\Pi(\alpha+\beta-\gamma)}{\Pi(\alpha-1) \Pi(\beta-1)}$$

Het behoeft nauwelijks gezegd te worden, dat de hier uitgedrukte eigenschappen ook onmiddellijk uit de herleiding der F-functie volgen. De formule (4) is afgeleid met de formules [82] op p. 209 en formule (5) is afgeleid met Gauss' Werke, Bd. III, terwijl de formule (5) ook afgeleid kan worden uit de formule [28], p. 217.

$$\frac{(a+n-1)(a_1+n-1)\dots(a_k+n-1)}{n(\beta_1+n-1)\dots(\beta_k+n-1)}x,$$

dan vindt men voor

$$u = a + a_1 + a_2 + \dots + a_k - \beta_1 - \beta_2 - \dots - \beta_k$$

$$\lim_{x=1} (1-x)^u F(x) = \frac{\Pi(u-1) \Pi(\beta_1-1) \Pi(\beta_2-1) \dots \Pi(\beta_k-1)}{\Pi(a-1) \Pi(a_1-1) \Pi(a_2-1) \dots \Pi(a_k-1)}$$

en wanneer

$$a + a_1 + a_2 + \dots + a_k - \beta_1 - \beta_2 - \dots - \beta_k = 0$$

is,

$$\lim_{x=1} \frac{F(x)}{\log\left(\frac{1}{1-x}\right)} = \frac{\Pi(\beta_1-1) \Pi(\beta_2-1) \dots \Pi(\beta_k-1)}{\Pi(a-1) \Pi(a_1-1) \dots \Pi(a_k-1)}$$

4. Neemt men in het theorema van art. 2 voor de functie  $F(x)$  het bijzonder

$$\psi(x) = \frac{1}{1-x} = 1 + x + x^2 + \dots,$$

zoodat

$$a_0 = a_1 = a_2 = \dots = a_n = 1,$$

dan volgt dus

$$\lim_{x=1} (1-x) \{s_0 + s_1 x + s_2 x^2 + \dots\} = M,$$

$$\lim_{n=\infty} s_n = M.$$

Het theorema, in art. 1 vermeld, is blijkbaar algemeen, wanneer  $\lim_{n=\infty} s_n = M$  is, zoo ziet men gemakkelijk, dat hi

$$\lim_{n=\infty} \frac{s_0 + s_1 + \dots + s_{n-1}}{n} = M,$$

terwijl men uit dit laatste niet omgekeerd tot  $\lim_{n=\infty} s_n = M$  kan overgaan.

Deze omstandigheid gaf aanleiding om te onderzoeken

$$\psi(x) = (1-x)^{-u} = 1 + \frac{u}{1}x + \frac{u(u+1)}{1 \cdot 2}x^2 + \dots$$

( $u > 0$ )

en voor

$$\psi(x) = \log\left(\frac{1}{1-x}\right) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \dots$$

Het bewijs zal hier alleen voor  $\psi(x) = (1-x)^{-u}$  daar het bewijs voor

$$\psi(x) = \log\left(\frac{1}{1-x}\right)$$

hierna geen bezwaar zal opleveren.

Uit de onderstelling, dat

$$\lim_{n \rightarrow \infty} \frac{s_0 + s_1 + \dots + s_{n-1}}{n} = M,$$

volgt, dat hoe klein een positief getal  $\varepsilon$  ook ge-  
mogelijk is een geheel positief getal  $n$  zoo groot

$$(6) \quad \dots \dots \dots \frac{s_0 + s_1 + \dots + s_{n+k-1}}{n+k} = M + \varepsilon$$

( $k = 0, 1, 2, 3, \dots$ )

de getallen  $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$  alle, volstrekt genomen

Zij nu verder

$$(7) \quad \begin{cases} P = s_0 + \frac{u}{1}s_1x + \frac{u(u+1)}{1 \cdot 2}s_2x^2 + \dots + \frac{u(u+1)}{1 \cdot 2 \cdot 3} \\ Q = 1 + \frac{u}{1}x + \frac{u(u+1)}{1 \cdot 2}x^2 + \dots + \frac{u(u+1)}{1 \cdot 2 \cdot 3} \end{cases}$$

terwijl ik er aan herinner, dat

$$f(x) = s_0 + \frac{u}{1}s_1x + \frac{u(u+1)}{1 \cdot 2}s_2x^2 + \dots$$

$$\psi(x) = 1 + \frac{u}{1}x + \frac{u(u+1)}{1 \cdot 2}x^2 + \dots =$$

convergeert. Met behulp van (7) en (8) kan men nu  $f(x)$  aldus voorstellen.

$$9) \quad \left\{ \begin{aligned} f(x) &= P + M\{(1-x)^{-u} - Q\} - n(u)_n \varepsilon_0 x^n + R + S, \\ R &= u(1-x) \sum_{k=1}^{k=\infty} (u+1)_{n+k-1} \varepsilon_k x^{n+k-1}, \\ S &= (1-u) \sum_{k=1}^{k=\infty} (u)_{n+k-1} \varepsilon_k x^{n+k-1}. \end{aligned} \right.$$

Hierin is ter bekorting door  $(u)_p$  de coëfficiënt van  $x^p$  in de ontwikkeling van  $(1-x)^{-u}$  aangeduid, dus

$$(u)_p = \frac{u(u+1) \dots (u+p-1)}{1 \cdot 2 \cdot 3 \dots p}.$$

Daar  $\varepsilon_1, \varepsilon_2, \dots$  alle, volstrekt genomen, kleiner dan  $\varepsilon$  zijn, zoo is de volstrekte waarde van R kleiner dan

$$\varepsilon u(1-x) \sum_{k=1}^{k=\infty} (u+1)_{n+k-1} x^{n+k-1},$$

en evenzoo de volstrekte waarde van S kleiner dan

$$\pm \varepsilon(1-u) \sum_{k=1}^{k=\infty} (u)_{n+k-1} x^{n+k-1}.$$

A fortiori zijn dus de volstrekte waarden van R en S respectievelijk kleiner dan

$$\varepsilon u(1-x) \sum_{k=0}^{k=\infty} (u+1)_k x^k = \varepsilon u(1-x)^{-u}$$

en

$$\pm \varepsilon(1-u) \sum_{k=0}^{k=\infty} (u)_k x^k = \pm \varepsilon(1-u)(1-x)^{-u}.$$

Stelt men dus

Uit (9) volgt dus nu, door vermenigvuldiging met  
 (11) .  $(1-x)^u f(x) = M + \{P - MQ - n(u)_{n\varepsilon_0} x^n\} (1-x)^u$

De functie  $P - MQ - n(u)_{n\varepsilon_0} x^n$  is geheel rationaal voor  $x=1$  noodzakelijk eene eindige waarde aan, z

$$\{P - MQ - n(u)_{n\varepsilon_0} x^n\} (1-x)^u,$$

daar  $u$  positief is, stellig tot nul convergeert, wanneer  $x$  naar 1 nemend, onbepaald tot de eenheid nadert. Men kan dus, als eene positieve grootheid  $\delta$  ook gegeven is, altijd  $\alpha$  bepalen zoodanig, dat voor alle waarden van  $x$  die  $1-\alpha \leq x < 1$  de volstrekte waarde van

$$\{P - MQ - n(u)_{n\varepsilon_0} x^n\} (1-x)^u$$

kleiner dan  $\delta$  is.

Het valt nu uit (11) gemakkelijk op te maken, dat  $(1-x)^u f(x)$ , bij onbeperkte nadering van  $x$  tot 1 convergeert, m. a. w. dat, hoe klein  $\beta$  ook gegeven is, men zoo kan bepalen, dat voor alle waarden van  $x$  die  $1-\alpha \leq x < 1$  de waarde van  $(1-x)^u f(x)$  minder van  $M$  afwijkt dan  $\beta$ . Inderdaad, men neme twee positieve getallen  $\delta$  en  $\varepsilon$

$$\beta = \delta + t\varepsilon.$$

Bij de waarde van  $\varepsilon$  bepale men nu  $n$  zóó, dat  $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$  in (6) allen volstrekt kleiner dan  $\varepsilon$  uitvalt, en daarmee ook  $P$  en  $Q$ , bekend zijn, bepale men  $\alpha$  zoodanig, dat, wanneer  $x$  niet meer dan  $\alpha$  van 1 afwijkt, de waarde van

$$\{P - MQ - n(u)_{n\varepsilon_0} x^n\} (1-x)^u$$

volstrekt kleiner dan  $\delta$  is. Volgens (11) ligt dan voor alle waarden van  $x$  het product  $(1-x)^u f(x)$  tusschen de grenzen  $M - \delta - t\varepsilon$ , d.i. tusschen  $M + \beta$  en  $M - \beta$ .

## VI.

(Amsterdam, Nieuw Arch Wisk, IX, 1882, 98—106.)

(traduction)

---

### A propos de quelques théorèmes concernant les séries infinies

1. Dans le 89<sup>ième</sup> tome du Journal für die reine und angewandte Mathematik, p 242—244, M. G. Frobenius publie dans un court article Ueber die Leibnizsche Reihe un théorème auquel il donne finalement la forme suivante:

„Si  $s_n$  est une fonction de  $n$  et que l'expression

$$\frac{s_0 + s_1 + \dots + s_{n-1}}{n}$$

tend vers une limite déterminée et finie lorsque  $n$  augmente, l'expression

$$(1-x)(s_0 + s_1 x + s_2 x^2 + s_3 x^3 + \dots)$$

tend vers la même limite lorsque la valeur de  $x$  tend vers l'unité en croissant continuellement.”

Ce théorème montre une certaine analogie avec un autre théorème qui m'était connue depuis longtemps et dont la vérité, à ce qu'il me paraît, s'impose pour peu qu'on y réfléchisse; pour cette raison j'en étais abstenu autrefois d'en chercher une démonstration achevée et rigoureuse. Cependant, l'article de M. Frobenius me fournit maintenant l'occasion de développer quelque peu mes idées à ce sujet et d'y ajouter quelques remarques qui font voir qu'on peut dire générale-

lorsque  $x$  tend vers l'unité en augmentant continuellement vers la même limite que l'expression

$$\frac{s_0 + s_1 + \dots + s_{n-1}}{n} \text{ pour } n = \infty.$$

Il me semble que la forme de la démonstration laisse rien à désirer; c'est pourquoi je n'ai pas l'entièrement sous ce rapport.

2. Le théorème dont je parlais est le suivant. Soient les grandeurs  $a_0, a_1, a_2, \dots$  soient toutes positives ou négatives et que la série

$$\psi(x) = a_0 + a_1 x + a_2 x^2 + \dots$$

converge pour toutes les valeurs de  $x$ , telles que  $x < 1$ , qu'elle diverge pour  $x = 1$ .

On en conclut aisément que la valeur de  $\psi(x)$  tend vers une certaine limite lorsque  $x$  tend vers 1 en croissant.

$$s_0, s_1, s_2, \dots$$

représentent une série illimitée de nombres convergents vers une limite  $M$  <sup>1)</sup>, il est évident que la série

$$f(x) = a_0 s_0 + a_1 s_1 x + a_2 s_2 x^2 + \dots$$

converge elle-aussi pour toutes les valeurs de  $x$ , telles que  $x < 1$ .

Or dans ces hypothèses la propriété qu'il s'agit de démontrer consiste en ce que l'expression

$$\frac{f(x)}{\psi(x)}$$

tend vers la limite  $M$ , lorsque  $x$  tend vers l'unité continuellement.

L'hypothèse faite à-propos de la série de nom

$$s_0, s_1, s_2, \dots$$

# QUELQUES THÉORÈMES CONCERNANT LES SÉRIES

$$(1) \quad \dots \dots \dots s_{n+k} = M + \varepsilon_k, \\ (k = 0, 1, 2, 3, \dots)$$

les nombres

$$\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$$

sont tous inférieurs à  $\varepsilon$  en valeur absolue.

Posons

$$(2) \quad \dots \dots \dots \begin{cases} P = a_0 s_0 + a_1 s_1 x + a_2 s_2 x^2 + \dots + a_{n-1} s_{n-1} x^{n-1} \\ Q = a_0 + a_1 x + a_2 x^2 + \dots + a_{n-1} x^{n-1} \end{cases}$$

On a alors, en faisant usage de l'équation (1),

$$f(x) = P + a_n x^n (M + \varepsilon_0) + a_{n+1} x^{n+1} (M + \varepsilon_1) + a_{n+2} x^{n+2} (M + \varepsilon_2) + \dots$$

Il s'ensuit que  $f(x)$  a une valeur intermédiaire entre

$$P + (M + \varepsilon) [\psi(x) - Q]$$

et

$$P + (M - \varepsilon) [\psi(x) - Q],$$

d'où l'on conclut que  $\frac{f(x)}{\psi(x)}$  a une valeur intermédiaire

$$M + \varepsilon + \frac{P - Q (M + \varepsilon)}{\psi(x)}$$

et

$$M - \varepsilon + \frac{P - Q (M - \varepsilon)}{\psi(x)}.$$

Or, lorsque  $x$  tend vers 1,  $P$  et  $Q$  tendent vers finies, tandis que  $\psi(x)$ , d'après notre hypothèse, augmente sans toute limite. Il sera donc possible de prendre  $\psi(x)$  inférieure à 1 et si peu différente de 1 qu'en va les expressions

$$\frac{P - Q (M + \varepsilon)}{\psi(x)} \quad \text{et} \quad \frac{P - Q (M - \varepsilon)}{\psi(x)}$$



$$\begin{aligned} \psi(x) &= a_0 + a_1 x + a_2 x^2 + \dots = (1-x)^{-u} \\ f(x) &= a_0 s_0 + a_1 s_1 x + a_2 s_2 x^2 + \dots = F(a, \beta, \gamma, x) \end{aligned}$$

et d'après (3)

$$\lim_{n \rightarrow \infty} s_n = M = \frac{\Pi(u-1) \Pi(\gamma-1)}{\Pi(\alpha-1) \Pi(\beta-1)},$$

de sorte qu'on obtient immédiatement

$$(4) \quad \lim_{x \rightarrow 1} (1-x)^{\alpha+\beta-\gamma} F(a, \beta, \gamma, x) = \frac{\Pi(\alpha+\beta-\gamma)}{\Pi(\alpha-1)}$$

$$II. \quad \alpha + \beta - \gamma = 0.$$

Si l'on pose, pour traiter ce cas,

$$\begin{aligned} s_0 &= \frac{1}{\alpha}, \quad s_n = \frac{(a+1)(a+2)\dots(a+n)\beta(\beta+1)\dots(\beta+n)}{1 \cdot 2 \cdot 3 \dots n \cdot \gamma(\gamma+1)\dots(\gamma+n)} \\ a_0 &= a, \quad a_n = \frac{\alpha}{n+1}, \end{aligned}$$

il en résulte

$$\begin{aligned} \psi(x) &= a + \frac{1}{2} a x + \frac{1}{3} a x^2 + \dots = \frac{a}{x} \log \left( \frac{1}{1-x} \right) \\ \lim_{n \rightarrow \infty} s_n &= \frac{\Pi(\gamma-1)}{\Pi(\alpha) \Pi(\beta-1)} = \frac{\Pi(\alpha+\beta-1)}{\alpha \Pi(\alpha-1) \Pi(\beta-1)} \end{aligned}$$

Et après une petite réduction on obtient

$$(5) \quad \lim_{x \rightarrow 1} \frac{F(a, \beta, \alpha+\beta, x)}{\log \left( \frac{1}{1-x} \right)} = \frac{\Pi(\alpha+\beta-1)}{\Pi(\alpha-1) \Pi(\beta-1)}$$

Il est presque superflu de dire que les propriétés (4) et (5) peuvent aussi être déduites immédiatement de la transformation de la fonction  $F$ . La formule (4) se trouve dans les formules [82], p. 209 et [48], p. 147 des Oeuvres de Gauss, tandis que la formule (5) est une conséquence immédiate de la formule [28], p. 217.

$$\frac{(a+n-1)(a_1+n-1)\dots(a_k+n-1)}{n(\beta_1+n-1)\dots(\beta_k+n-1)}x,$$

on trouve pour

$$u = a + a_1 + a_2 + \dots + a_k - \beta_1 - \beta_2 - \dots - \beta_k > 0$$

$$\lim_{x=1} (1-x)^u F(x) = \frac{\Pi(u-1)\Pi(\beta_1-1)\Pi(\beta_2-1)\dots\Pi(\beta_k-1)}{\Pi(a-1)\Pi(a_1-1)\Pi(a_2-1)\dots\Pi(a_k-1)}$$

et pour

$$a + a_1 + a_2 + \dots + a_k - \beta_1 - \beta_2 - \dots - \beta_k = 0$$

$$\lim_{x=1} \frac{F(x)}{\log\left(\frac{1}{1-x}\right)} = \frac{\Pi(\beta_1-1)\Pi(\beta_2-1)\dots\Pi(\beta_k-1)}{\Pi(a-1)\Pi(a_1-1)\dots\Pi(a_k-1)}.$$

4. Si dans le théorème du n° 2 on donne à  $\psi(x)$  la form

$$\psi(x) = \frac{1}{1-x} = 1 + x + x^2 + \dots,$$

de sorte que

$$a_0 = a_1 = a_2 = \dots = a_n = 1,$$

il s'ensuit que

$$\lim_{x=1} (1-x)\{s_0 + s_1x + s_2x^2 + \dots\} = M,$$

$$\lim_{n=\infty} s_n = M.$$

Le théorème énoncé au n° 1 est évidemment plus général pour  $\lim_{n=\infty} s_n = M$  on peut en tirer, comme cela se voit aisément

$$\lim_{n=\infty} \frac{s_0 + s_1 + \dots + s_{n-1}}{n} = M,$$

tandis qu'il n'est pas possible de tirer réciproquement de la première équation la formule  $\lim_{n=\infty} s_n = M$ .

Cette circonstance m'induisit à examiner si d'autres h

$$\psi(x) = (1-x)^{-u} = 1 + \frac{u}{1}x + \frac{u(u+1)}{1 \cdot 2}x^2 + \dots$$

$(u > 0)$

et

$$\psi(x) = \log\left(\frac{1}{1-x}\right) = x + \frac{1}{2}x^2 + \frac{1}{3}x^3 + \dots$$

Je ne donnerai la démonstration que pour  $\psi(x) = \log\left(\frac{1}{1-x}\right)$  que la démonstration pour

$$\psi(x) = \log\left(\frac{1}{1-x}\right)$$

n'offre ensuite aucune difficulté.

De l'hypothèse

$$\lim_{n \rightarrow \infty} \frac{s_0 + s_1 + \dots + s_{n-1}}{n} = M,$$

on déduit qu'il est toujours possible, quelque nombre positif donné  $\varepsilon$ , de prendre un nombre que pour

$$(6) \quad \dots \dots \dots \frac{s_0 + s_1 + \dots + s_{n+k-1}}{n+k} = M + \varepsilon$$

$(k = 0, 1, 2, 3, \dots)$

les nombres  $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$  deviennent tous inférieurs à

Posons ensuite

$$(7) \quad \begin{cases} P = s_0 + \frac{u}{1}s_1x + \frac{u(u+1)}{1 \cdot 2}s_2x^2 + \dots + \frac{u(u+1)\dots}{1 \cdot 2 \cdot 3 \dots}x^{n-1} \\ Q = 1 + \frac{u}{1}x + \frac{u(u+1)}{1 \cdot 2}x^2 + \dots + \frac{u(u+1)\dots}{1 \cdot 2 \cdot 3 \dots}x^{n-1} \end{cases}$$

je puis rappeler qu'on a

$$f(x) = s_0 + \frac{u}{1}s_1x + \frac{u(u+1)}{1 \cdot 2}s_2x^2 + \dots,$$

A l'aide des équations (7) et (8) on peut maintenant donner à  $f$  la forme suivante :

$$(9) \quad \left\{ \begin{array}{l} f(x) = P + M [(1-x)^{-u} - Q] - n(u)_n \varepsilon_0 x^n + R + S, \\ R = u(1-x) \sum_{k=1}^{k=\infty} (u+1)_{n+k-1} \varepsilon_k x^{n+k-1}, \\ S = (1-u) \sum_{k=1}^{k=\infty} (u)_{n+k-1} \varepsilon_k x^{n+k-1}. \end{array} \right.$$

Pour plus de brièveté on a appelé ici  $(u)_p$  le coefficient de  $x^p$  dans le développement de  $(1-x)^{-u}$ , c. à. d. on a pris

$$(u)_p = \frac{u(u+1) \dots (u+p-1)}{1 \cdot 2 \cdot 3 \dots p}.$$

Attendu que les grandeurs  $\varepsilon_1, \varepsilon_2, \dots$  sont toutes en valeur absolue inférieures à  $\varepsilon$ , la valeur absolue de  $R$  est inférieure à

$$\varepsilon u(1-x) \sum_{k=1}^{k=\infty} (u+1)_{n+k-1} x^{n+k-1},$$

et de même la valeur absolue de  $S$  est inférieure à

$$\pm \varepsilon(1-u) \sum_{k=1}^{k=\infty} (u)_{n+k-1} x^{n+k-1}.$$

A plus forte raison les expressions  $R$  et  $S$  sont donc, en valeur absolue, inférieures à

$$\varepsilon u(1-x) \sum_{k=0}^{k=\infty} (u+1)_k x^k = \varepsilon u(1-x)^{-u}$$

et

$$\pm \varepsilon(1-u) \sum_{k=0}^{k=\infty} (u)_k x^k = \pm \varepsilon(1-u)(1-x)^{-u}$$

respectivement.

où  $y$  représente une fraction positive ou négative.

L'équation (9) donne maintenant, après multi-

$$(11) \quad (1-x)^u f(x) = M + \{P - MQ - n(u)_n \varepsilon_0 x^n\} (1-x)^u$$

La fonction  $P - MQ - n(u)_n \varepsilon_0 x^n$  est rationnelle et prend toujours une valeur finie pour  $x=1$ , de sorte que

$$\{P - MQ - n(u)_n \varepsilon_0 x^n\} (1-x)^u$$

attendu que  $u$  a une valeur positive, tend vers zéro lorsque  $x$  se rapproche indéfiniment de l'unité. On conclut donc que  $(1-x)^u f(x)$  tend vers  $M$  uniformément.

On peut donc toujours, quelque petite que soit la valeur positive donnée  $\delta$ , déterminer un nombre positif  $\alpha$  tel que pour toutes les valeurs de  $x$  satisfaisant à  $1-\alpha < x < 1$ , la valeur de l'expression

$$\{P - MQ - n(u)_n \varepsilon_0 x^n\} (1-x)^u$$

devienne inférieure à  $\delta$  en valeur absolue.

Or, on déduit aisément de l'équation (11) que  $(1-x)^u f(x)$  tend réellement vers la limite  $M$ , lorsque  $x$  se rapproche de l'unité, en d'autres termes qu'on peut toujours trouver, que soit une grandeur donnée  $\beta$ , déterminer un nombre  $\alpha$  tel que pour toutes les valeurs de la variable satisfaisant à  $1-\alpha < x < 1$ , la différence entre la valeur de  $(1-x)^u f(x)$  et  $M$  devienne inférieure à  $\beta$ .

En effet, prenez deux nombres positifs  $\delta$  et  $\varepsilon$ .

$$\beta = \delta + t \varepsilon.$$

Déterminez ensuite le nombre  $n$  de telle manière que, d'après la relation (6) les valeurs de  $\varepsilon_0, \varepsilon_1, \varepsilon_2, \dots$  deviennent inférieures en valeur absolue, inférieures à celle de  $\varepsilon$ . Le nombre  $n$  étant ainsi connu, prenez un nombre  $\alpha$  tel que pour toutes les valeurs de  $x$  et l'unité n'est pas supérieure à  $\alpha$ , l'expression

## VII.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, III—

### Over de transformatie van de periodieke functiën

$$A_0 + A_1 \cos \varphi + B_1 \sin \varphi + \dots + A_n \cos n \varphi + B_n \sin n \varphi$$

Het groote nut, dat men in veel gevallen kan trekken uit de ontbinding in factoren van eene uitdrukking van bovengenoemde vorm, schijnt mij de volgende eenvoudige ontwikkeling van deze uitdrukking hierop betrekking heeft te wettigen.

Voor het geval, dat  $n=2$  is, en de uitdrukking voor geëlimineerd van  $\varphi$  gelijk aan 0 wordt, heeft men deze ontbinding in factoren bij de ontwikkeling der storingsfunctie sedert lang toegepast. art. 54 van de Auseinandersetzung einer zweckmässigen Methode zur Berechnung der absoluten Störungen der kleinen Planeten. Abhandlung, zegt Hansen in eene noot: Die allgemeine Theorie der Auflösung des Polynomen

$$X = \gamma_0 + \gamma_1 \cos x + \gamma_2 \cos 2x + \gamma_3 \cos 3x + \dots \\ + \sin x \cdot \{\beta_0 + \beta_1 \cos x + \beta_2 \cos 2x + \dots\}$$

in Factoren habe ich in meiner Pariser Preisschrift vollstellig bewerkstelligt. Ik heb van de hier aangevoerde Mémoire, sur les perturbations qu'éprouvent les comètes, geen inzage kunnen krijgen.

Omtrent de reële coëfficiënten  $A_k, B_k$ , in de

$$A_0 + A_1 \cos \varphi + A_2 \cos 2 \varphi + \dots + A_n \cos n \varphi \\ + B_1 \sin \varphi + B_2 \sin 2 \varphi + \dots + B_n \sin n \varphi$$

zal alleen ondersteld worden, dat  $A_n$  en  $B_n$  niet nul zijn, wat blijkbaar geen schade aan de algemeene bekorting zal bovenstaande uitdrukking door  $F(\varphi)$  zij verder

$$e^{\varphi i} = \cos \varphi + i \sin \varphi = z,$$

dus

$$e^{-\varphi i} = \cos \varphi - i \sin \varphi = z^{-1}$$

dan is

$$2 F(\varphi) = 2 A_0 + A_1 (z + z^{-1}) + A_2 (z^2 + z^{-2}) + \dots \\ - B_1 i (z - z^{-1}) - B_2 i (z^2 - z^{-2}) - \dots$$

of wel

$$2 z^n F(\varphi) = G(z),$$

wanneer gesteld wordt

$$G(z) = (A_n - B_n i) z^{2n} + (A_{n-1} - B_{n-1} i) z^{2n-1} + \dots + (A_0 + B_0 i) \\ + (A_1 + B_1 i) z^{n-1} + (A_2 + B_2 i) z^{n-2} + \dots$$

De gebroken functie  $\frac{1}{2} z^{-n} G(z)$  neemt dus voor waarden van  $z$  met den modulus 1, de waarde der geheele functie van den  $2n^{\text{den}}$  graad  $G(z)$  heeft als eigenschap, dat

$$z^{2n} G\left(\frac{1}{z}\right)$$

toegevoegd is met  $G(z)$ , en dit heeft eene bijzondere beteekenis, want de wortels der vergelijking  $G(z) = 0$  ten gevolge

$$G(z) = (A_n - B_n i) (z - p_1 e^{q_1 i}) (z - p_2 e^{q_2 i}) \dots$$

dan moet de uitdrukking rechts eveneens

vergelijking  $G(z) = 0$ , elk dezer wortels zooveel maal neergeschreven als door den graad van veelvoudigheid wordt aangewezen,

$$p_1 e^{q_1 i}, p_2 e^{q_2 i}, \dots, p_{2n} e^{q_{2n} i},$$

en volgens de tweede ontbinding

$$\frac{1}{p_1} e^{q_1 i}, \frac{1}{p_2} e^{q_2 i}, \dots, \frac{1}{p_{2n}} e^{q_{2n} i}.$$

Daar nu deze beide groepen alleen in volgorde kunnen verschillen zoo blijkt hieruit, dat wanneer  $p_1 e^{q_1 i}$  een  $r$ -voudige wortel is, ook  $\frac{1}{p_1} e^{q_1 i}$  een  $r$ -voudige wortel is.

De gezamenlijke wortels van de vergelijking  $G(z) = 0$  kunnen dus in twee groepen gesplitst worden.

Vooreerst de wortels met een modulus verschillend van 1. Deze wortels kunnen voorgesteld worden door

$$r_1 e^{u_1 i}, r_2 e^{u_2 i}, \dots, r_k e^{u_k i}, \\ \frac{1}{r_1} e^{u_1 i}, \frac{1}{r_2} e^{u_2 i}, \dots, \frac{1}{r_k} e^{u_k i},$$

waarin  $r_1, r_2, \dots, r_k$  alle kleiner dan 1 zijn.

Het geheele aantal dezer wortels is even en gelijk aan  $2k$ .

Ten tweede de wortels met een modulus 1. Deze mogen zijn

$$e^{v_1 i}, e^{v_2 i}, \dots, e^{v_{2l} i}.$$

Hun aantal  $2l$  is evenzeer even, en men heeft

$$k + l = n.$$

Het is trouwens duidelijk, dat  $v_1, v_2, \dots, v_{2l}$  de wortels zijn van  $F(\varphi) = 0$ ,

en daar  $F(\varphi)$ , bij vermeerdering van  $\varphi$  met  $2\pi$ , dezelfde waarde aanneemt, zoo valt hieruit reeds op te maken, dat het aantal dezer wortels even moet zijn.

Hierbij is nog op te merken, dat uit

$$2\pi n F(\omega) = G(z)$$



waaruit blijkt, dat wanneer voor zekere waarde

$$G(z), G'(z), G''(z), \dots, G^{(r-1)}(z)$$

alle nul worden, en  $G^{(r)}(z)$  niet nul is, voor welke waarde van  $\varphi$  ook

$$F(\varphi), F'(\varphi), F''(\varphi), \dots, F^{(r-1)}(\varphi)$$

gelijk nul zijn, en  $F^{(r)}(\varphi)$  niet nul is; zoodat een waarde van  $G(z)=0$  overeenkomt met een  $r$ -voudigen waarde van  $\varphi$ .

Wat  $u_1, u_2, \dots, u_k, v_1, v_2, \dots, v_{2l}$  betreft, wegens de exponentiaalfunctie kan men elk dezer waarden  $u_i$  veelvoud van  $2\pi$  vermeerderen of verminderen met een geheel getal, bijv.  $>0$  en  $<2\pi$  onderstellen. Het is voor het geheel onverschillig, hoe de bepaling hierover gekozen wordt, zoodat men steeds aanneemt dat  $0 \leq u_i < 2\pi$  en  $0 \leq v_i < 2\pi$ . Neer slechts aan de eenmaal aangenomen waarde van  $\varphi$  wordt.

Na dit alles is dus

$$G(z) = (A_n - B_n i) \times T \times U \times V,$$

$$T = (z - r_1 e^{u_1 i}) \dots (z - r_k e^{u_k i})$$

$$U = \left(z - \frac{1}{r_1} e^{u_1 i}\right) \dots \left(z - \frac{1}{r_k} e^{u_k i}\right)$$

$$V = (z - e^{v_1 i}) (z - e^{v_2 i}) \dots (z - e^{v_{2l} i})$$

en dus voor  $z = e^{i\varphi}$

$$F(\varphi) = \frac{1}{2} e^{-n\varphi i} (A_n - B_n i) \times T \times U \times V$$

Door nu de factoren van  $T, U, V$  respectievelijk

$$e^{i\varphi} - r_1 e^{u_1 i} = e^{u_1 i} \times (e^{(\varphi - u_1) i} - r_1),$$

$$e^{i\varphi} - \frac{1}{r_1} e^{u_1 i} = e^{i\varphi} \times \left(1 - \frac{1}{r_1} e^{-(\varphi - u_1) i}\right),$$

$$F(\varphi) = C [1 - 2r_1 \cos(\varphi - u_1) + r_1^2] \times \dots \times [1 - 2r_k \cos(\varphi - u_k) + r_k^2] \times \\ \times \sin \frac{1}{2}(\varphi - v_1) \sin \frac{1}{2}(\varphi - v_2) \dots \sin \frac{1}{2}(\varphi - v_{2l}),$$

waarin

$$C = (-1)^n 2^{2l-1} (A_n - B_n i) e^{\frac{1}{2}(v_1 + v_2 + \dots + v_{2l} + 2u_1 + 2u_2 + \dots + 2u_k)i} (r_1 r_2 \dots r_k)^{-1}$$

Bepaalt men  $R$  en  $\alpha$  zoodanig, dat

$$A_n + B_n i = R e^{\alpha i},$$

dus

$$A_n - B_n i = R e^{-\alpha i}$$

is, dan volgt voor het product van alle wortels der vergelijking

$G(z) = 0$  de waarde  $e^{2\alpha i}$ , dus

$$e^{2\alpha i} = e^{(v_1 + v_2 + \dots + v_{2l} + 2u_1 + 2u_2 + \dots + 2u_k)i},$$

of wel

$$2\alpha + 2m\pi = v_1 + v_2 + \dots + v_{2l} + 2u_1 + 2u_2 + \dots + 2u_k,$$

waarin  $m$  een geheel getal is, waarvan de waarde door deze vergelijking volkomen bepaald wordt, wanneer men eenmaal de waarden van  $v_1, v_2, \dots, v_{2l}, u_1, u_2, \dots, u_k$  en  $\alpha$  op bepaalde wijze aangenomen heeft.

De waarde van  $C$  wordt nu

$$(-1)^n 2^{2l-1} R e^{-\alpha i} e^{\alpha + m\pi} (r_1 r_2 \dots r_k)^{-1},$$

of

$$C = (-1)^{m+n} 2^{2l-1} R (r_1 r_2 \dots r_k)^{-1}.$$

Hier volgt ten slotte de samenstelling van alle formules:

$$F(\varphi) = A_0 + A_1 \cos \varphi + A_2 \cos 2\varphi + \dots + A_n \cos n\varphi + \\ + B_1 \sin \varphi + B_2 \sin 2\varphi + \dots + B_n \sin n\varphi,$$

$$G(z) = (A_n - B_n i) z^{2n} + (A_{n-1} - B_{n-1} i) z^{2n-1} + \dots + (A_1 - B_1 i) z^{n+1} + \\ + 2A_0 z^n + (A_1 + B_1 i) z^{n-1} + (A_2 + B_2 i) z^{n-2} + \dots + (A_n + B_n i).$$

$$A_n + B_n i = R e^{a i},$$

$$2\alpha + 2m\pi = v_1 + v_2 + \dots + v_{2l} + 2(u_1 + u_2 + \dots + u_{2l}),$$

$$C = (-1)^{m+n} 2^{2l-1} R (r_1 r_2 \dots r_k) \dots$$

$$F(\varphi) = C \times \prod_{p=1}^{p=k} [1 - 2r_p \cos(\varphi - u_p) + r_p^2] \times \prod_{p=1}^{p=2l} [1 - 2r_p \cos(\varphi - u_p) + r_p^2]$$

Om een enkel voorbeeld te geven, zij

$$F(\varphi) = 4 - 3\sqrt{2} \sin \varphi - 2\sqrt{2} \cos^3 \varphi$$

Men vindt, dat  $F(\varphi)$ ,  $F'(\varphi)$ ,  $F''(\varphi)$  voor  $\varphi = 45^\circ$  wijl  $F'''(\varphi)$  niet nul is, dus heeft men

$$v_1 = v_2 = v_3 = 45^\circ.$$

Een vierden wortel van  $F(\varphi) = 0$  vindt men door te zoeken, komt

$$v_4 = 106^\circ 35' 45''.4.$$

Nadat aldus vier wortels van de zesdemachtsvergelijking gevonden zijn, is het gemakkelijk de beide overige wortels te bepalen. Ik verkrijg ten slotte

$$F(\varphi) = C [1 - 2r \cos(\varphi - u) + r^2] \sin^3 \frac{1}{2}(\varphi - v_1) \sin^3 \frac{1}{2}(\varphi - v_4)$$

$$^{10}\log C = 1.268505,$$

$$^{10}\log r = 9.484070 - 16,$$

$$u = 239^\circ 12' 7''.3,$$

$$v_1 = 45^\circ,$$

$$v_4 = 106^\circ 35' 45''.4.$$

## VII.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, 111—116)

(traduction)

---

### De la transformation de la fonction périodique

$$A_0 + A_1 \cos \varphi + B_1 \sin \varphi + \dots + A_n \cos n\varphi + B_n \sin n\varphi.$$

La grande utilité qu'on peut retirer dans bien des cas de la décomposition en facteurs d'une expression de la forme écrite ci-dessus me semble justifier les simples considérations suivantes sur ce sujet.

Dans le cas où  $n=2$  et où cette expression ne devient nulle pour aucune valeur de  $\varphi$  on a depuis longtemps appliqué cette décomposition en facteurs; on s'en est servi dans le développement de la fonction perturbatrice, et dans le n<sup>o</sup>. 54 de son Auseinandersetzung einer zweckmässigen Methode zur Berechnung der absoluten Störungen der kleineren Planeten, erste Abhandlung, Hansen dit dans une note: J'ai développé complètement dans mon ouvrage couronné à Paris la théorie générale de la décomposition en facteurs du polynôme

$$\begin{aligned} X = \gamma_0 + \gamma_1 \cos x + \gamma_2 \cos 2x + \gamma_3 \cos 3x + \dots \\ + \sin x \cdot \{ \beta_0 + \beta_1 \cos x + \beta_2 \cos 2x + \dots \}. \end{aligned}$$

Je n'ai pas pu me procurer le Mémoire sur les perturbations qu'éprouvent les comètes, auquel l'auteur fait allusion; et la forme dans laquelle Hansen pose le problème pourrait nous amener à supposer que sa méthode diffère quelque peu de la nôtre.

est celle ci que  $A_n$  et  $B_n$  ne s'annulent pas en même temps pas à la généralité.

Pour simplifier, l'expression ci-dessus sera indiquée en outre

$$e^{q^1} = \cos q + i \sin q = z,$$

donc

$$e^{-q^1} = \cos q - i \sin q = z^{-1},$$

nous avons alors

$$\begin{aligned} 2F(q) = & 2A_0 + A_1(z + z^{-1}) + A_2(z^2 + z^{-2}) + \dots + A_n(z^n + z^{-n}) \\ & - B_1 i(z - z^{-1}) - B_2 i(z^2 - z^{-2}) - \dots - B_n i(z^n - z^{-n}) \end{aligned}$$

ou bien

$$2z^n F(q) = G(z),$$

si l'on pose

$$\begin{aligned} G(z) = & (A_n - B_n i) z^{2n} + (A_{n-1} - B_{n-1} i) z^{2n-1} + \dots + (A_1 - B_1 i) z^{n+1} \\ & + (A_1 + B_1 i) z^{n-1} + (A_2 + B_2 i) z^{n-2} + \dots + (A_n + B_n i) \end{aligned}$$

La fonction fractionnaire  $\frac{1}{2} z^{-n} G(z)$  prend donc pour des valeurs de  $z$  dont le module est égal à l'unité. La fonction entière  $G(z)$  du degré  $2n$  jouit apparemment de la propriété suivante : l'expression

$$z^{2n} G\left(\frac{1}{z}\right)$$

est conjuguée avec  $G(z)$ . Il en résulte une certaine propriété de l'équation  $G(z) = 0$ . En effet, posons

$$G(z) = (A_n - B_n i)(z - p_1 e^{q_1}) (z - p_2 e^{q_2}) \dots (z - p_n e^{q_n})$$

L'expression qui figure au second membre doit alors être conjuguée avec elle-même lorsque l'on remplace  $z$  par  $\frac{1}{z}$ , qu'on multiplie ensuite par  $z^{2n}$  et qu'on change enfin  $i$  en  $-i$ . Par conséquent

multiplicité correspondant; et d'après la seconde décomposition elles sont

$$\frac{1}{p_1} e^{q_1 i}, \frac{1}{p_2} e^{q_2 i}, \dots, \frac{1}{p_{2n}} e^{q_{2n} i}.$$

Comme ces deux groupes ne peuvent différer que par l'ordre de leurs termes, il s'ensuit que lorsque  $p_1 e^{q_1 i}$  est  $r$  fois racine, il en est de même pour  $\frac{1}{p_1} e^{q_1 i}$ .

Les racines de l'équation  $G(z) = 0$  peuvent donc être divisées en deux groupes.

On a d'abord les racines dont le module diffère de l'unité. Ces racines peuvent être représentées par les expressions

$$r_1 e^{u_1 i}, \quad r_2 e^{u_2 i}, \dots, r_k e^{u_k i}, \\ \frac{1}{r_1} e^{u_1 i}, \quad \frac{1}{r_2} e^{u_2 i}, \dots, \frac{1}{r_k} e^{u_k i},$$

où les grandeurs  $r_1, r_2, \dots, r_k$  sont toutes inférieures à l'unité.

Le nombre total de ces racines est pair et égal à  $2k$ .

En second lieu nous avons les racines avec un module 1. Supposons que ce soient les racines

$$e^{v_1 i}, \quad e^{v_2 i}, \dots, \quad e^{v_{2l} i}.$$

Leur nombre  $2l$  est pair également, et l'on a

$$k + l = n.$$

Il est d'ailleurs évident que  $v_1, v_2, \dots, v_{2l}$  sont les racines de

$$F(\varphi) = 0$$

et comme  $F(\varphi)$ , lorsque l'angle  $\varphi$  est augmenté de  $2\pi$ , prend la même valeur, cette remarque suffit pour faire voir que le nombre de ces racines doit être pair.

Nous pouvons encore observer à ce sujet que l'équation

$$2z^n F(\varphi) = G(z)$$

ce qui fait voir que lorsque pour une valeur déterminée de  $z$  les fonctions

$$G(z), G'(z), G''(z), \dots, G^{(r-1)}(z)$$

s'annulent toutes, tandis que  $G^{(r)}(z)$  ne s'annule pas.

$$F(\varphi), F'(\varphi), F''(\varphi), \dots, F^{(r-1)}(\varphi)$$

s'annulent également pour la valeur correspondante de  $\varphi$ . Si  $F^{(r)}(\varphi)$  ne s'annule pas: d'où il résulte qu'un nombre  $\varphi$  qui est une racine de  $G(z)=0$  correspond à un nombre qui n'est pas une racine de  $F(\varphi)=0$ .

Quant à  $u_1, u_2, \dots, u_k, v_1, v_2, \dots, v_{2l}$ , à cause de la fonction exponentielle, on peut augmenter ou diminuer ces grandeurs d'un multiple quelconque de  $2\pi$ . On peut les supposer toutes p. e.  $> 0$  et  $< 2\pi$ . Il est complètement indifférent pour la suite de savoir quelle chose on a fait: il suffit qu'on s'en tienne aux valeurs adoptées.

Après tout ceci on a donc

$$G(z) = (A_n - B_n i) \times T \times U \times V,$$

$$T = (z - r_1 e^{u_1 i}) \dots (z - r_k e^{u_k i}),$$

$$U = \left(z - \frac{1}{r_1} e^{u_1 i}\right) \dots \left(z - \frac{1}{r_k} e^{u_k i}\right),$$

$$V = (z - e^{v_1 i}) (z - e^{v_2 i}) \dots (z - e^{v_{2l} i}),$$

partant, pour  $z = e^{\varphi i}$

$$F(\varphi) = \frac{1}{2} e^{-n\varphi i} (A_n - B_n i) \times T \times U \times V.$$

En réduisant alors les facteurs de  $T$ , de  $U$  et de  $V$  de la manière suivante

$$e^{\varphi i} - r_1 e^{u_1 i} = e^{u_1 i} \times (e^{(\varphi - u_1) i} - r_1),$$

$$e^{\varphi i} - \frac{1}{r_1} e^{u_1 i} = e^{\varphi i} \times \left(1 - \frac{1}{r_1} e^{-(\varphi - u_1) i}\right),$$

on obtient

$$F(\varphi) = C [1 - 2r_1 \cos(\varphi - u_1) + r_1^2] \times \dots \times [1 - 2r_k \cos(\varphi - u_k) + r_k^2] \times \\ \times \sin \frac{1}{2}(\varphi - v_1) \sin \frac{1}{2}(\varphi - v_2) \dots \sin \frac{1}{2}(\varphi - v_{2l});$$

où

$$C = (-1)^n 2^{2l-1} (A_n - B_n i) e^{\frac{1}{2}(v_1 + v_2 + \dots + v_{2l} + 2u_1 + 2u_2 + \dots + 2u_k)i} (r_1 r_2 \dots r_k)^{-1}$$

Si l'on détermine  $R$  et  $\alpha$  de telle manière que

$$A_n + B_n i = R e^{\alpha i},$$

donc

$$A_n - B_n i = R e^{-\alpha i},$$

on obtient pour le produit de toutes les racines de l'équation

$G(z) = 0$  la valeur  $e^{2\alpha i}$  et par conséquent

$$e^{2\alpha i} = e^{(v_1 + v_2 + \dots + v_{2l} + 2u_1 + 2u_2 + \dots + 2u_k)i}$$

ou bien

$$2\alpha + 2m\pi = v_1 + v_2 + \dots + v_{2l} + 2u_1 + 2u_2 + \dots + 2u_k;$$

équation dans laquelle  $m$  représente un nombre entier, dont la valeur est entièrement déterminée par cette équation, dès qu'on a adopté des valeurs déterminées de  $v_1, v_2, \dots, v_{2l}$ , de  $u_1, u_2, \dots, u_k$  et de  $\alpha$ .

La valeur de  $C$  devient maintenant

$$(-1)^n 2^{2l-1} R e^{-\alpha i} e^{(\alpha + m\pi)i} (r_1 r_2 \dots r_k)^{-1},$$

ou

$$C = (-1)^{m+n} 2^{2l-1} R (r_1 r_2 \dots r_k)^{-1}.$$

Voici enfin une récapitulation de toutes les formules trouvées:

$$F(\varphi) = A_0 + A_1 \cos \varphi + A_2 \cos 2\varphi + \dots + A_n \cos n\varphi + \\ + B_1 \sin \varphi + B_2 \sin 2\varphi + \dots + B_n \sin n\varphi,$$

$$G(z) = (A_n - B_n i) z^{2n} + (A_{n-1} - B_{n-1} i) z^{2n-1} + \dots + (A_1 - B_1 i) z^{n+1} + \\ + 2A_0 z^n + (A_1 + B_1 i) z^{n-1} + (A_2 + B_2 i) z^{n-2} + \dots + (A_n + B_n i).$$

Les racines de  $G(z) = 0$  sont



$$A_n + B_n i = R e^{a i},$$

$$2a + 2m\pi = v_1 + v_2 + \dots + v_{2l} + 2(u_1 + u_2 + \dots + u_{2l}),$$

$$C = (-1)^{m+n} 2^{2l-1} R (r_1 r_2 \dots r_k)^{-1},$$

$$F(\varphi) = C \times \prod_{p=1}^{p=k} [1 - 2r_p \cos(\varphi - u_p) + r_p^2] \times \prod_{p=1}^{p=2l} \sin \frac{1}{2}(\varphi - v_p)$$

Pour donner un seul exemple, soit

$$F(\varphi) = 4 - 3\sqrt{2} \sin \varphi - 2\sqrt{2} \cos^3 \varphi.$$

On trouve que  $F(\varphi)$ ,  $F'(\varphi)$ ,  $F''(\varphi)$  s'annulent pour  $\varphi = 0$ ,  
 $F'''(\varphi)$  ne s'annule pas. Donc

$$v_1 = v_2 = v_3 = 45^\circ.$$

Une quatrième racine de  $F(\varphi) = 0$ , trouvée par d'approximation, est

$$v_4 = 106^\circ 35' 45'' .4.$$

Après que quatre racines de l'équation du sixième ont été trouvées de cette manière, il est facile de trouver les deux autres  $r e^{u i}$  et  $\frac{1}{r} e^{u i}$ . J'obtiens enfin

$$F(\varphi) = C [1 - 2r \cos(\varphi - u) + r^2] \sin^3 \frac{1}{2}(\varphi - v_1) \sin \frac{1}{2}(\varphi - v_4)$$

$${}^{10}\log C = 1.268505,$$

$${}^{10}\log r = 9.484070 - 16,$$

$$u = 239^\circ 12' 7'' .3,$$

$$v_1 = 45^\circ,$$

$$v_4 = 106^\circ 35' 45'' .4.$$

## VIII.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, 198—211)

---

### Over een algorithmus voor het meetkundig midden.

In het 89<sup>ste</sup> deel van het Journal für die reine und angewandte Mathematik p. 343, heb ik eene rekenwijze aangegeven, waardoor het mogelijk is, wanneer  $k$  positieve getallen  $a_1, a_2, \dots, a_k$  gegeven zijn, uit deze getallen op rationale wijze  $k$  andere getallen  $b_1, b_2, \dots, b_k$  af te leiden, zoodanig dat  $a_1 a_2 \dots a_k = b_1 b_2 \dots b_k$  is, en de verschillen tusschen de getallen  $b_1, b_2, \dots, b_k$  onderling zoo klein kunnen zijn als men verkiest.

Ik stel mij voor in het volgende op dit onderwerp terug te komen, en de bewijzen mede te deelen van hetgeen in die korte noot is uitgesproken.

1. Zij dan, wanneer  $a_1, a_2, \dots, a_k$  willekeurige reële getallen zijn  $M_1$  hun rekenkundig midden, d. w. z. hun som gedeeld door hun aantal  $k$ ;  $M_2$  het rekenkundig midden van alle producten van twee verschillende der getallen  $a_1, a_2, \dots, a_k$ , d. w. z. de som dezer producten gedeeld door hun aantal  $\frac{k(k-1)}{2}$ ; evenzoo  $M_3$  het rekenkundig midden van alle producten van drie verschillende der getallen  $a_1, a_2, \dots, a_k$  enz; eindelijk  $M_k = a_1 a_2 \dots a_k$ .

Voor de gelijkvormigheid stel ik nog vast,  
De uitdrukking

$$M_p^2 - M_{p-1} M_{p+1} \\ (p = 1, 2, 3, \dots, k-1)$$

is nu in het algemeen positief, of scherper uitgedrukt, is nooit negatief en alleen dan gelijk nul, als de tallen  $a_1, a_2, \dots, a_k$  aan elkander gelijk zijn, of als  $k-p+1$  dezer getallen gelijk nul zijn, in welk geval  $M_{p-1}$  en  $M_{p+1}$  afzonderlijk gelijk nul zijn.

Deze eigenschap is in hoofdzaak sedert lang bekend. Zie eenige geschiedkundige opmerkingen hieromtrent in de Bijlagen met te verwijzen naar een opstel van Dr. D. B. van der Waerden in het 8<sup>ste</sup> deel der Verslagen en mededeelingen der Koninklijke Academie van Wetenschappen, Afdeeling Natuurkunde, 1858, p. 248—260. Men zie ook het opstel van Dr. D. B. van der Waerden in het 9<sup>de</sup> deel dier Verslagen, p. 92—106.

Voor het gemak van den lezer, en ook om de duidelijkheid waarin de uitdrukking gelijk nul wordt, volkomen te laten zien, laat ik hier echter het bewijs van het boven gezegde.

2. Zij gegeven

$$(1) \quad \begin{cases} f(x) = (x - a_1)(x - a_2) \dots (x - a_k) \\ f(x) = M_0 x^k - \frac{k}{1} M_1 x^{k-1} + \frac{k(k-1)}{1 \cdot 2} M_2 x^{k-2} - \dots \end{cases}$$

waar in het tweede lid het bovenste of onderste lid is, al naar dat  $k$  even of oneven is.

Volgens de onderstelling omtrent  $a_1, a_2, \dots, a_k$  is de gelijkning  $f(x) = 0$  slechts reële wortels, en hetzelve geldt van de vergelijkingen, die vorderen, dat de verschillenden  $a_i$  van  $f(x)$  de waarde nul aannemen. Daarom heeft

Ik onderscheid nu deze drie gevallen.

1°.  $M_{p+1}$  is niet gelijk nul.

2°.  $M_{p+1} = 0$ , maar  $M_p$  is niet gelijk nul.

3°.  $M_{p+1} = 0$  en  $M_p = 0$ .

In het eerste geval zijn ook alle wortels van de vergelijking

$$(3) \quad 0 = M_{p+1}x^{p+1} - \frac{p+1}{1} M_p x^p + \frac{p(p+1)}{1 \cdot 2} M_{p-1} x^{p-1} \dots \pm \frac{p!}{1 \cdot 2 \cdot \dots \cdot p} M_0$$

reëel, en derhalve ook die van

$$(4) \quad \dots \dots \dots 0 = M_{p+1}x^2 - 2M_p x + M_{p-1};$$

want het tweede lid dezer laatste vergelijking onderscheidt zich alleen door een standvastigen factor van de  $(p-1)^{\text{ste}}$  afgeleide functie, die het tweede lid van (3) uitmaakt. Uit de wortels van (4) volgt nu

$$M_p^2 - M_{p-1} M_{p+1} \geq 0;$$

en wel is  $M_p^2 - M_{p-1} M_{p+1}$  alleen dan gelijk nul, wanneer alle wortels van (4) gelijk zijn. Hiertoe is weder noodzakelijk dat alle wortels van (3), dus ook alle wortels van (4), onderling elkaar gelijk zijn, wat weder medebrengt dat alle wortels van  $f(x) = 0$  gelijk zijn, of  $a_1 = a_2 = \dots = a_k$ .

Is dus  $M_{p+1}$  niet gelijk nul, dan is  $M_p^2 - M_{p-1} M_{p+1}$  altijd positief behalve wanneer  $a_1 = a_2 = \dots = a_k$ , in welk geval de uitdrukking gelijk aan nul is.

In het tweede geval is blijkbaar  $M_p^2 - M_{p-1} M_{p+1}$  positief.

Eindelijk is in het derde geval deze uitdrukking gelijk nul, en heeft de vergelijking (2) minstens twee wortels gelijk nul. De vergelijking  $f(x) = 0$  minstens  $k - p + 1$  wortels gelijk nul, of m. a. w. in dit geval zijn minstens  $k - p + 1$  der getallen  $a_1, a_2, \dots, a_k$  gelijk aan nul.

zoodat de getroffen overeenkomst omtrent  $M_0$  ver

$$a'_p = \frac{M_p}{M_{p-1}},$$

$$(p = 1, 2, 3, \dots, k)$$

waaruit volgt

$$a'_p - a'_{p+1} = \frac{M_p^2 - M_{p-1} M_{p+1}}{M_{p-1} M_p}$$

dus

$$a'_p \geq a'_{p+1};$$

en, wanneer ook de waarde nul voor  $a_1, a_2, \dots$ , kan alleen dan  $a'_1 = a'_{p+1}$  worden, wanneer  $a_1 =$  ook dit laatste geval geheel zonder belang is, buiten beschouwing blijven, en is derhalve

$$(6) \quad \dots \quad a'_1 > a'_2 > a'_3 > a'_4 > \dots > a'_k$$

terwijl uit (5) onmiddellijk volgt

$$(7) \quad \dots \quad a_1 a_2 a_3 \dots a_k = a'_1 a'_2 a'_3 \dots a'_k.$$

Nu is blijkbaar

$$a'_1 = \frac{a_1 + a_2 + a_3 + \dots + a_k}{k}$$

$$a'_k = \frac{k}{\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \dots + \frac{1}{a_k}}$$

en, wanneer wij nu onderstellen dat geen der  $a$  groter dan  $a_1$  en kleiner dan  $a_k$  is, zoo volgt

$$a'_1 \leq \frac{(k-1)a_1 + a_k}{k} < a_1,$$

$$a'_k > a_1,$$

evenzoo uit  $a_1'', a_2'', \dots, a_k''$  de getallen  $a_1''', a_2''', \dots, a_k'''$  enz; dan is du

$$a_1 > a_1' > a_2' > \dots > a_k' > a_k,$$

$$a_1' > a_1'' > a_2'' > \dots > a_k'' > a_k',$$

$$a_1'' > a_1''' > a_2''' > \dots > a_k''' > a_k'',$$

$$\dots \dots \dots$$

$$0 < a_1' - a_k' < \frac{k-1}{k} (a_1 - a_k),$$

$$0 < a_1'' - a_k'' < \frac{k-1}{k} (a_1' - a_k') < \left(\frac{k-1}{k}\right)^2 (a_1 - a_k),$$

$$0 < a_1''' - a_k''' < \frac{k-1}{k} (a_1'' - a_k'') < \left(\frac{k-1}{k}\right)^3 (a_1 - a_k),$$

$$\dots \dots \dots$$

$$a_1 a_2 \dots a_k = a_1' a_2' \dots a_k' = a_1'' a_2'' \dots a_k'' = a_1''' a_2''' \dots a_k''' = \dots,$$

en voor de  $n^{\text{de}}$  afgeleide groep van getallen  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  heet  
men

$$a_1^{(n-1)} > a_1^{(n)} > a_2^{(n)} > \dots > a_k^{(n)} > a_k^{(n-1)},$$

$$0 < a_1^{(n)} - a_k^{(n)} < \left(\frac{k-1}{k}\right)^n (a_1 - a_k),$$

$$a_1 a_2 \dots a_k = a_1^{(n)} a_2^{(n)} \dots a_k^{(n)}.$$

Daar nu

$$\left(\frac{k-1}{k}\right)^n$$

bij onbepaald toenemende waarden van  $n$ , ten slotte zoo klein word  
als men verkiest, zoo volgt dat de getallen  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  all  
voor  $n = \infty$  tot eene gemeenschappelijke limiet convergeeren, di

Eerste voorbeeld.  $k=3$ .

$$\begin{aligned} a_1 &= 5, & a_2 &= 5, & a_3 &= 5, \\ a'_1 &= \frac{14}{3}, & a'_2 &= \frac{65}{14}, & a'_3 &= \frac{17}{14}, \\ a''_1 &= \frac{7603}{1638}, & a''_2 &= \frac{35290}{7673}, & a''_3 &= \frac{17}{14}, \end{aligned}$$

of

$$\begin{aligned} a''_1 &= 4.64163\ 61416\ 36\dots \\ a''_2 &= 4.64158\ 88465\ 08\dots \\ a''_3 &= 4.64154\ 15131\ 77\dots \end{aligned}$$

Men ziet, hoe snel de getallen van een naderen, immers

$$\begin{aligned} a'_1 - a'_2 &= 0.02380\ 95\dots \\ a'_2 - a'_3 &= 0.02747\ 25\dots \\ a''_1 - a''_2 &= 0.00004\ 72951\dots \\ a''_2 - a''_3 &= 0.00004\ 73333\dots \end{aligned}$$

Het gemiddelde der waarden van de twee

$$a''_1 = 4.64158\ 88337\ 74\dots$$

Later zal blijken, dat het verschil  $a''_1 - a''_2$  de 10<sup>de</sup> decimaal bedraagt. De limiet is hi

$$\sqrt[3]{100} = 4.64158\ 88336\ 1276\dots$$

Tweede voorbeeld.  $k=4$ .

$$\begin{aligned} a_1 &= 3, & a_2 &= 2, & a_3 &= 2, & a_4 &= 2, \\ a'_1 &= \frac{9}{4}, & a'_2 &= \frac{20}{9}, & a'_3 &= \frac{1}{5}, & a'_4 &= \frac{1}{5}, \\ a''_1 &= \frac{17531}{7920}, & a''_2 &= \frac{116410}{52593}, & a''_3 &= \frac{1}{5}, & a''_4 &= \frac{1}{5}, \end{aligned}$$

en

$$a'_1 - a'_2 = 0.02777\ 78 \dots,$$

$$a'_2 - a'_3 = 0.02222\ 22 \dots,$$

$$a'_3 - a'_4 = 0.01118\ 18 \dots,$$

$$a''_1 - a''_2 = 0.00009\ 76697\ 0 \dots,$$

$$a''_1 - a''_3 = 0.00009\ 74240\ 1 \dots,$$

$$a''_3 - a''_4 = 0.00009\ 71786\ 0 \dots$$

Uit de waarden van  $a'_1, a'_2, a'_3, a'_4$  volgt

$$a'''_1 = 2.21336\ 38420\ 8 \dots;$$

de limiet is hier

$$\sqrt[4]{24} = 2.21336\ 38394\ 007 \dots$$

5. In de beide gegeven voorbeelden worden de verschillen der opvolgende getallen van eene zelfde groep

$$a'_1 - a'_2, a'_2 - a'_3, \dots$$

$$a''_1 - a''_2, a''_2 - a''_3, \dots$$

niet alleen bij overgang tot de volgende groepen, hoe langer hoe kleiner, maar de verschillen die tot eene zelfde groep behooren, worden hierbij onderling hoe langer hoe minder verschillend.

Inderdaad kan men het volgende uitspreken.

Het quotiënt van elke twee der  $k-1$  verschillen

$$\frac{a_p^{(n)} - a_{p+1}^{(n)}}{(p=1, 2, 3, \dots, k-1)}$$

convergeert voor  $n = \infty$  tot de limiet 1.

Van de verschillende bewijzen, die ik voor deze eigenschap vond is het volgende verreweg het eenvoudigste.

6. Ik stel

$$a_1 = a - x_1,$$

$$a_2 = a - x_2,$$



$$(9) \quad \begin{cases} f(x) = (x - x_1)(x - x_2) \dots (x - x_k), \\ f(x) = N_0 x^k - \frac{k}{1} N_1 x^{k-1} + \frac{k(k-1)}{1 \cdot 2} N_2 x^{k-2} - \dots \end{cases}$$

zoodat de getallen  $N_0, N_1, \dots, N_k$  op dezelfde wijze  
 vormd zijn als  $M_0, M_1, \dots, M_k$  uit  $a_1, a_2, \dots$ ,  
 onduidelijkheid aanleiding geven, dat  $f(x)$  hier  
 andere beteekenis heeft dan in art. 2. Men  
 middellijk, dat de getallen  $M_0, M_1, \dots, M_k$ , op  
 middel van de functie  $f(x)$  en hare afgeleiden  
 kunnen worden

$$(10) \quad \begin{cases} M_k = \\ k M_{k-1} = \\ k(k-1) M_{k-2} = \\ \dots \\ k(k-1) \dots 3 \cdot 2 M_1 = \\ k(k-1) \dots 3 \cdot 2 \cdot 1 M_0 = \end{cases}$$

waaruit dus volgt

$$(11) \quad \dots \dots \dots \alpha'_p = \frac{p f^{k-p}(a)}{f^{k-p+1}(a)},$$

$$(p = 1, 2, 3, \dots, k)$$

waarbij  $f^0(a) = f(a)$  te nemen is.

In plaats van (11) kan men ook schrijven

$$(12) \quad \alpha'_p = \frac{N_0 a^p - \frac{p}{1} N_1 a^{p-1} + \frac{p(p-1)}{1 \cdot 2} N_2 a^{p-2} - \dots}{N_0 a^{p-1} - \frac{(p-1)}{1} N_1 a^{p-2} + \frac{(p-1)(p-2)}{1 \cdot 2} N_2 a^{p-3} - \dots}$$

Ontwikkelt men deze waarde van  $\alpha'_p$  volgens  
 van  $a$ , dan vindt men voor de eerste termen

Evenzoo mogen  $z_1 < z_2 < \dots < z_{p-1}$  de reële ongelijke wortels van de vergelijking  $f^{k-p+1}(x) = 0$  zijn, zoodat  $z_1$  tusschen  $y_1$  en  $y_2$ ,  $z_2$  tusschen  $y_2$  en  $y_3 \dots$ , eindelijk  $z_{p-1}$  tusschen  $y_{p-1}$  en  $y_p$  ligt. Hierbij is dus  $p > 1$  te onderstellen. Volgens (11) is dan

$$a'_p = \frac{(a - y_1)(a - y_2) \dots (a - y_p)}{(a - z_1)(a - z_2) \dots (a - z_{p-1})},$$

en wanneer men de deeling uitvoert en in gedeeltelijke breuken splits, volgens (13)

$$(14) \quad \dots \quad a'_p = a - N_1 + \sum_{k=1}^{p-1} \frac{A_k}{a - z_k},$$

waarin

$$(15) \quad \dots \quad A_k = \frac{(z_k - y_1)(z_k - y_2) \dots (z_k - y_p)}{(z_k - z_1) \dots (z_k - z_{k-1})(z_k - z_{k+1}) \dots (z_k - z_{p-1})}.$$

In den teller van deze uitdrukking voor  $A_k$  zijn de factoren

$$(z_k - y_1)(z_k - y_2) \dots (z_k - y_k),$$

alle positief; daarentegen de overige factoren, ten getale van  $p - k$

$$z_k - y_{k+1}, z_k - y_{k+2}, \dots, z_k - y_p,$$

alle negatief.

De negatieve factoren in den noemer van  $A_k$  zijn

$$z_k - z_{k+1}, z_k - z_{k+2}, \dots, z_k - z_{p-1};$$

hun aantal is  $p - k - 1$ . Het aantal negatieve factoren in den teller van  $A_k$  is dus één grooter dan het aantal negatieve factoren in den noemer; derhalve zijn

$$A_1, A_2, A_3, \dots, A_{p-1},$$

alle negatief, en daar de verschillen

$$a - z_1 > a - z_2 > \dots > a - z_{k-1}$$

positief zijn, zoo volgt

volgens (13) gelijk aan  $-(p-1)(N_1^2 - N_0 N_2)$ , verder dan  $a - x_1 = a_1$ ,  $a - z_{p-1}$  grooter dan  $a - x_k =$  blijkbaar gelijk aan  $a'_1$  is; zoodat nu volgt

$$(16) \quad \dots \quad \left\{ \begin{array}{l} a'_p < a'_1 - \frac{(p-1)(N_1^2 - N_0 N_2)}{a_1}, \\ a'_p > a'_1 - \frac{(p-1)(N_1^2 - N_0 N_2)}{a_k}. \end{array} \right.$$

Voor  $p=1$  heeft men blijkbaar de teekens  $\dots$  gelijke tekenen te vervangen.

7. De afleiding der ongelijkheden (16) steunt wistandigheid dat  $A_1, A_2, \dots, A_{p-1}$  alle negatief zijn laatste ook nog aldus aantoonen.

Zij

$$g(x) = (x - y_1)(x - y_2) \dots (x - y_p)$$

dan is blijkbaar

$$a'_p = \frac{p g(a)}{g'(a)},$$

en

$$\frac{g'(x)}{g(x)} = \frac{1}{x - y_1} + \frac{1}{x - y_2} + \dots + \frac{1}{x - y_p}$$

waaruit door differentiatie volgt

$$\frac{g(x) g''(x) - g'(x) g'(x)}{g(x) g(x)} = -\frac{1}{(x - y_1)^2} - \frac{1}{(x - y_2)^2} - \dots$$

en men vindt, hierin  $x = z_k$  stellende, daar  $g'(z_k)$

$$\frac{g''(z_k)}{g(z_k)} = -\frac{1}{(z_k - y_1)^2} - \frac{1}{(z_k - y_2)^2} - \dots$$

Nu is echter, zooals uit  $a'_p = \frac{p g(a)}{g'(a)}$  onmiddellijk

$$A_k = \frac{p g(z_k)}{g''(z_k)}$$

$$a'_p - a'_{p+1} < \frac{a_k + p(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2),$$

$$a'_p - a'_{p+1} > \frac{a_1 - p(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2),$$

us daar  $p$  hoogstens gelijk is aan  $k-1$  en  $a_1 - a_k$  en  $N_1^2 - N_0 N_2$  positief zijn, zoo veel te meer

$$17) \quad \dots \quad \left\{ \begin{array}{l} a'_p - a'_{p+1} < \frac{a_k + (k-1)(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2) \\ a'_p - a'_{p+1} > \frac{a_1 - (k-1)(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2). \end{array} \right.$$

In de uitdrukking rechts komt nu  $p$  niet meer voor.

Al de voorgaande ontwikkelingen blijven onveranderd, wanneer men de getallen  $a_1, a_2, \dots, a_k$ , door  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  en tegelijkertijd  $a'_1, a'_2, \dots, a'_k$  door  $a_1^{(n+1)}, a_2^{(n+1)}, \dots, a_k^{(n+1)}$  vervangt.

Daar nu reeds bewezen is, dat  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  voor  $n = \infty$  tot eene zelfde positieve limiet naderen, zoo kan men blijkbaar  $n$  altijd groot nemen, dat

$$a_1^{(n)} - (k-1)(a_1^{(n)} - a_k^{(n)})$$

positief is, en dan volgt gemakkelijk

$$18) \quad \frac{a_1^{(n)} - (k-1)(a_1^{(n)} - a_k^{(n)})}{a_k^{(n)} + (k-1)(a_1^{(n)} - a_k^{(n)})} < \frac{a_p^{(n+1)} - a_{p+1}^{(n+1)}}{a_q^{(n+1)} - a_{q+1}^{(n+1)}} < \frac{a_k^{(n)} + (k-1)(a_1^{(n)} - a_k^{(n)})}{a_1^{(n)} - (k-1)(a_1^{(n)} - a_k^{(n)})}$$

Neemt men  $n$  groot genoeg, dan verschillen de beide waarden waartusschen

$$\frac{a_p^{(n+1)} - a_{p+1}^{(n+1)}}{a_q^{(n+1)} - a_{q+1}^{(n+1)}}$$

ligt, zoo weinig als men verkiest van de eenheid.

Hiermede is dus het in art 5 uitgesprokene bewezen.

of

$$k \left( \frac{1}{b_1} + \frac{1}{b_2} + \dots + \frac{1}{b_k} \right) (b'_1 - b'_k) = 1 + \frac{b_2}{b_1} + \frac{b_3}{b_1} + \frac{b_4}{b_1} + \dots + \frac{b_k}{b_1} + 1 + \frac{b_3}{b_2} + \frac{b_4}{b_2} + \dots + \frac{b_k}{b_2} + 1 + \frac{b_4}{b_3} + \frac{b_5}{b_3} + \dots + \frac{b_k}{b_3} + \dots + \frac{b_k}{b_k} + \frac{b_{k+1}}{b_k} + \dots$$

De uitdrukking rechts is

$$= \Sigma \left( \frac{b_p}{b_q} + \frac{b_q}{b_p} - 2 \right) = \Sigma \frac{(b_p - b_q)^2}{b_p b_q},$$

waar  $p$  en  $q$  de getallen  $1, 2, 3, \dots, k$  doorloopen.

Deelt men nu beide leden door  $(b_1 - b_k)^2$  en neemt de limiet voor  $n = \infty$ , dan volgt, daar volgens h

$$\lim_{n=\infty} \frac{(b_p - b_q)^2}{(b_1 - b_k)^2} = \left( \frac{p - q}{k - 1} \right)^2$$

is, en ter bekorting de limiet van  $b_1, b_2, \dots, b_k$  g

$$\frac{k^2}{b} \lim_{n=\infty} \frac{b'_1 - b'_k}{(b_1 - b_k)^2} = \frac{1}{(k-1)^2 b^2} \Sigma (p -$$

Nu is

$$\begin{aligned} \Sigma (p - q)^2 &= 1^2 + 2^2 + 3^2 + \dots + (k-1)^2 \\ &\quad + 1^2 + 2^2 + \dots + (k-2)^2 \\ &\quad + 1^2 + \dots + (k-3)^2 \\ &\quad \dots \end{aligned}$$

waarvoor men na herleiding verkrijgt

$$\Sigma (p - q)^2 = \frac{1}{12} k^2 (k^2 - 1),$$

10. Deze formule (19) geeft een duidelijk begrip van de snelheid waarmede ten slotte de getallen tot hunne gemeenschappelijke limiet  $\sqrt[k]{a_1 a_2 \dots a_k}$  convergeeren; het blijkt dat  $a_1^{(n+1)} - a_k^{(n+1)}$  eene eindige verhouding heeft tot de tweede macht van  $a_1^{(n)} - a_k^{(n)}$ .

In het eerste voorbeeld van art. 4 was

$$a_1'' - a_3'' = 0.00009\ 4628 \dots,$$

en als benaderde waarde van  $a_1''' - a_3'''$  kan nu genomen worden

$$\frac{1}{6} \frac{(a_1'' - a_3'')^2}{a_2''};$$

en daar  $a_1'''$ ,  $a_2'''$ ,  $a_3'''$  op zeer weinig na eene rekenkundige reek vormen, heeft men aan

$$a_1''' = 4.64158\ 88337\ 74 \dots$$

de correctie

$$-\frac{1}{12} \frac{(a_1'' - a_3'')^3}{a_2''} = -0.00000\ 00001\ 61 \dots$$

te voegen, om de in 12 decimalen nauwkeurige waarde van  $\sqrt[3]{10}$

$$4.64158\ 88336\ 13 \dots$$

te verkrijgen.

In het tweede voorbeeld heeft men aan

$$a_1''' = 2.21336\ 38420\ 8 \dots$$

de correctie

$$-\frac{5}{72} \frac{(a_1'' - a_4'')^2}{a_1''} = -0.00000\ 00026\ 8 \dots$$

aan te brengen, om te verkrijgen

$$\sqrt[3]{24} = 2.21336\ 38394\ 0 \dots$$

dan zijn blijkbaar  $M_0, M_1, M_2, \dots, M_h$  positief, en  $M_{h+1}, \dots, M_k$  alle gelijk nul.

Derhalve worden

$$a'_1, a'_2, \dots, a'_h$$

alle positief en niet gelijk nul,  $a'_{h+1} = 0$ ; terwijl bepaalde beteekenis hebben. Stelt men echter van  $a'_{h+1}, \dots, a'_k$  allen gelijk nul zullen zijn, dan zijn er

$$a'_1, a'_2, \dots, a'_k$$

evenveel gelijk nul, als van de oorspronkelijke  $a_1, a_2, \dots, a_k$ .

Men ziet nu onmiddellijk, dat de verdere betrekkingen art. 3 met hoogst geringe wijzigingen onveranderd blijven. Het is dus ook nu de getallen  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  tot een limiet gelijk aan nul is, convergeeren.

Daarentegen is de wijze, waarop deze convergentie plaats vindt, geheel anders, en men kan zeggen, dat de convergentie veel langzamer is.

Het blijkt namelijk, dat de verhouding van opeenvolgende getallen

$$a_p, a'_p, a''_p, a'''_p, \dots, a_p^{(n)} \dots$$

$$(p = 1, 2, 3, \dots, h)$$

bij toenemende  $n$  tot eene eindige, gemakkelijk te bepalen limiet convergeert, die voor de verschillende waarden van  $p$  verschillend is, terwijl de verhoudingen der getallen van eene ze

$$a_1^{(n)}, a_2^{(n)}, \dots, a_h^{(n)}$$

tot eindige limieten convergeeren, die alleen van de verhoudingen niet van de getallenwaarden van  $a_1, a_2, \dots, a_h$ , willekeurig gekozen, afgegaan.

Daar het strenge bewijs van deze eigenschap

die, zoo zij door  $a_1, a_2, \dots, a_k$  vervuld worden, voldoende zijn om te besluiten, dat de rekenwijze tot eene bepaalde limiet voert, en dan aan te geven, welke der  $k$  waarden van  $(a_1 a_2 \dots a_k)^{\frac{1}{k}}$  deze limiet is; maar het schijnt uiterst bezwaarlijk om, zoo  $a_1, a_2, \dots, a_k$  willekeurig gegeven zijn, uit te maken, of er al dan niet eene limiet is en in het eerste geval deze limiet aan te geven.

Alleen het geval  $k=2$  levert niet het minste bezwaar op, en het zal daarom voldoende zijn, de volgende uitkomsten eenvoudig mede te deelen.

Men vindt dan, dat in dit geval er altijd eene limiet gelijk aan

$$\pm \sqrt{a_1 a_2}$$

is, behalve wanneer de verhouding  $a_1 : a_2$  reëel negatief is.

Stelt men

$$a_1 = r_1 e^{a_1 i},$$

$$a_2 = r_2 e^{a_2 i},$$

en neemt  $r_1$  en  $r_2$  positief,  $a_1$  en  $a_2$  tusschen 0 en  $2\pi$  (de eerste waarde in-, de tweede buitengesloten), dan is de limiet gelijk aan

$$+ \sqrt{r_1 r_2} e^{\frac{1}{2}(a_1 + a_2)i},$$

wanneer de volstreckte waarde van  $a_1 - a_2$  kleiner dan  $\pi$  is.

Is echter  $a_1 - a_2$  grooter dan  $\pi$ , dan is de limiet gelijk aan

$$- \sqrt{r_1 r_2} e^{\frac{1}{2}(a_1 + a_2)i}.$$

Neemt men bijv.

$$a_1 = z, a_2 = \frac{1}{z},$$

dan is de limiet gelijk aan  $+1$  of  $-1$ , al naar dat het reële deel van  $z$  positief of negatief is.

Daar

$$a_1, a'_1, a''_1, a'''_1 \dots$$



convergeerend voor alle waarden van  $z$ , waarvan het reële deel gelijk nul is, en waarvan de som gelijk aan  $+1$  is, al naar dat het reële deel van  $z$  positief of negatief is.

Eene dergelijke reeks is door Weierstrass opgegeven in zijn belangrijke verhandeling zur Functionenlehre, veröffentlicht in den Monatsberichte der Königl. Preuss. Akademie der Wissenschaften, 1880, p. 735.

Kort daarna merkte Tannery op, dat men ook op andere wijze dergelijke reeksen kan vormen. (Zie Monatsberichte, 1881, p. 228 e. v.).

Men zal gemakkelijk opmerken, dat de bovenstaande reeks zonder geval begrepen is onder degene, die Weierstrass op pag. 230 aangeeft. (Men verbeterde daar de drukfout).

$$x' = \frac{1+x}{1-x} \text{ moet gelezen worden } x' = \frac{1-x}{1+x}.$$

Eene vertaling van het eerste opstel van Weierstrass is mededeeling naar aanleiding van Tannery's opmerking in het Bulletin des sciences mathématiques et astronomiques, 3<sup>e</sup> série, tome V, Avril 1881.

---

## VIII.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, 198—211.)

(traduction)

---

### Sur un algorithme de la moyenne géométrique.

Dans le 89<sup>ième</sup> tome du Journal für die reine und angewandte Mathematik, p. 343, j'ai indiqué une méthode de calcul permettant, lorsque  $k$  nombres positifs  $a_1, a_2, \dots, a_k$  sont donnés, d'en déduire rationnellement  $k$  autres nombres  $b_1, b_2, \dots, b_k$  de telle manière qu'on ait  $a_1 a_2 \dots a_k = b_1 b_2 \dots b_k$  et que les différences des nombres  $b_1, b_2, \dots, b_k$  soient aussi petites qu'on veut.

Je me propose de retourner sur ce sujet dans l'article présent et de faire connaître les preuves de ce qui a été avancé dans cette brève note.

1. Soient  $a_1, a_2, \dots, a_k$  des nombres réels arbitraires,  $M_1$  leur moyenne arithmétique, c. à. d. leur somme divisée par leur nombre  $k$ ;  $M_2$  la moyenne arithmétique de tous les produits différents des nombres  $a_1, a_2, \dots, a_k$  pris deux-à-deux, c. à. d. la somme de ces produits divisée par leur nombre  $\frac{k(k-1)}{2}$ ; de même  $M_3$  la moyenne arithmétique de tous les produits différents des nombres  $a_1, a_2, \dots, a_k$

rents; nous avons simplement voulu attribuer à chaque cas une individualité distincte

Pour des raisons de symétrie je pose encore  $M_0 =$

$$M_p^2 - M_{p-1} M_{p+1} \\ (p = 1, 2, 3, \dots, k-1)$$

est généralement positive ou, plus précisément, cette expression est toujours jamais négative et ne devient nulle que lorsque  $a_1, a_2, \dots, a_k$  sont égaux entre eux ou qu'au moins deux de ces nombres s'annulent auquel cas les expressions s'annulent évidemment l'une et l'autre.

Cette propriété générale est connue depuis longtemps. D'histoire il suffit de renvoyer le lecteur à un article de D. Bierens de Haan publié dans le 8<sup>ième</sup> tome des *Mededeelingen der Koninklijke Akademie van Wetenschappen* de physique, Amsterdam 1858, p. 248—260. Voir aussi l'article de Lobatto dans le 9<sup>ième</sup> tome des *Verslagen*.

Cependant pour épargner de la peine au lecteur et pour traiter d'une façon générale les cas limites où l'expression s'annule, je fais suivre ici la preuve du théorème

## 2. Posons

$$(1) \quad \begin{cases} f(x) = (x - a_1)(x - a_2) \dots (x - a_k) \\ f(x) = M_0 x^k - \frac{k}{1} M_1 x^{k-1} + \frac{k(k-1)}{1 \cdot 2} M_2 x^{k-2} - \dots \end{cases}$$

où il faut prendre dans le second membre le signe + ou le signe inférieur selon que le nombre  $k$  est pair ou impair.

D'après l'hypothèse faite au sujet des nombres  $a_1, a_2, \dots, a_k$  l'équation  $f(x) = 0$  n'a que des racines réelles et la même équation est vraie pour les équations exprimant que les dérivées de  $f(x)$  s'annulent. C'est pourquoi l'équation

Je distingue les trois cas suivants.

1°.  $M_{p+1}$  diffère de zéro.

2°.  $M_{p+1} = 0$ , mais  $M_p$  diffère de zéro.

3°.  $M_{p+1} = 0$  et  $M_p = 0$ .

Dans le premier cas les racines de l'équation

$$(3) \quad 0 = M_{p+1}x^{p+1} - \frac{p+1}{1}M_p x^p + \frac{p(p+1)}{1.2}M_{p-1}x^{p-1} \dots \pm \frac{p+1}{1}M_1x \pm M_0$$

sont toutes réelles, et il en est donc de même de celles de l'équation

$$(4) \quad \dots \dots \dots 0 = M_{p+1}x^2 - 2M_p x + M_{p-1};$$

en effet, le second membre de cette dernière équation ne diffère qu'

par un facteur constant de la  $(p-1)^{\text{ième}}$  dérivée de la fonction qu'

constitue le second membre de l'équation (3). De la réalité des racines

de (4) on conclut à l'inégalité

$$M_p^2 - M_{p-1}M_{p+1} \geq 0;$$

l'expression  $M_p^2 - M_{p-1}M_{p+1}$  ne s'annule que lorsque les deux racines

de l'équation (4) sont égales entre elles. A cet effet il faut et il

suffit que toutes les racines de (3), donc aussi toutes celles de (2)

soient égales entre elles, d'où l'on conclut que toutes les racines de

l'équation  $f(x) = 0$  sont égales entre elles, c. à d. que  $a_1 = a_2 = \dots = a_k$ .

Par conséquent lorsque  $M_{p+1}$  ne s'annule pas, l'expression

$M_p^2 - M_{p-1}M_{p+1}$  est toujours positive, excepté au cas où  $a_1 = a_2 = \dots = a_k$ .

car alors elle s'annule.

Dans le deuxième cas l'expression  $M_p^2 - M_{p-1}M_{p+1}$  est évidemment

positive.

Enfin dans le troisième cas cette expression est nulle et l'équation

(2) a au moins deux racines nulles, de sorte que l'équation  $f(x) =$

a au moins  $k - p + 1$  racines nulles; en d'autres termes, dans ce

cas au moins  $k - p + 1$  des nombres  $a_1, a_2, \dots, a_k$  s'annulent.

Nous venons de donner la démonstration complète du théorème

ces équations jointes à l'hypothèse faite au sujet de  $M_0$  me permettent d'écrire

$$a'_p = \frac{M_p}{M_{p-1}}.$$

$$(p = 1, 2, 3, \dots, k)$$

Il s'ensuit que

$$a'_p - a'_{p+1} = \frac{M_p^2 - M_{p-1} M_{p+1}}{M_{p-1} M_p},$$

donc

$$a'_p \geq a'_{p+1},$$

et si l'on exclut aussi la valeur 0 des nombres  $a_1, a_2$  peut avoir  $a'_1 = a'_{p+1}$ , à moins que  $a_1 = a_2 = \dots =$  dernier cas n'a lui aussi aucune importance nous pourrions convenir l'écart; nous avons donc

$$(6) \quad \dots \dots \dots a'_1 > a'_2 > a'_3 > a'_4 > \dots > a'_k,$$

tandis qu'on tire immédiatement des équations (5):

$$(7) \quad \dots \dots \dots a_1 a_2 a_3 \dots a_k = a'_1 a'_2 a'_3 \dots a'_k.$$

Or, on a évidemment

$$a'_1 = \frac{a_1 + a_2 + a_3 + \dots + a_k}{k},$$

$$a'_k = \frac{k}{\frac{1}{a_1} + \frac{1}{a_2} + \frac{1}{a_3} + \dots + \frac{1}{a_k}};$$

et si nous supposons qu'aucun des nombres  $a_1, a_2$ , supérieur à  $a_1$  ni inférieur à  $a_k$ , il s'ensuit que

$$a'_1 \leq \frac{(k-1)a_1 + a_k}{k} < a_1,$$

$$a'_k > a_1,$$

des nombres  $a_1, a_2, \dots, a_k$  nous avons déduit les nombres  $a'_1, a'_2, \dots, a'_k$ ,  
 et si des nombres  $a'_1, a'_2, \dots, a'_k$  nous déduisons de la même ma-  
 nière les nombres  $a''_1, a''_2, \dots, a''_k$ , etc., nous avons donc

$$a_1 > a'_1 > a'_2 > \dots > a'_k > a_k,$$

$$a'_1 > a''_1 > a''_2 > \dots > a''_k > a'_k,$$

$$a''_1 > a'''_1 > a'''_2 > \dots > a'''_k > a''_k,$$

$$\dots \dots \dots$$

$$0 < a'_1 - a'_k < \frac{k-1}{k} (a_1 - a_k),$$

$$0 < a''_1 - a''_k < \frac{k-1}{k} (a'_1 - a'_k) < \left(\frac{k-1}{k}\right)^2 (a_1 - a_k),$$

$$0 < a'''_1 - a'''_k < \frac{k-1}{k} (a''_1 - a''_k) < \left(\frac{k-1}{k}\right)^3 (a_1 - a_k),$$

$$\dots \dots \dots$$

$$a_1 a_2 \dots a_k = a'_1 a'_2 \dots a'_k = a''_1 a''_2 \dots a''_k = a'''_1 a'''_2 \dots a'''_k = \dots$$

Les équations correspondantes pour le  $n^{\text{ième}}$  groupe de nombres déduit  
 des groupes précédents, c. à. d. pour les nombres  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$ , sont

$$a_1^{(n-1)} > a_1^{(n)} > a_2^{(n)} > \dots > a_k^{(n)} > a_k^{(n-1)},$$

$$0 < a_1^{(n)} - a_k^{(n)} < \left(\frac{k-1}{k}\right)^n (a_1 - a_k),$$

$$a_1 a_2 \dots a_k = a_1^{(n)} a_2^{(n)} \dots a_k^{(n)}.$$

Or, comme l'expression

$$\left(\frac{k-1}{k}\right)^n,$$

lorsque  $n$  augmente indéfiniment, finit par devenir aussi petite qu'on  
 le désire, il s'ensuit que les nombres  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  convergent

Premier exemple.  $k = 3$ .

$$\begin{aligned} a_1 &= 5, & a_2 &= 5, & a_3 &= 4, \\ a'_1 &= \frac{14}{3}, & a'_2 &= \frac{65}{14}, & a'_3 &= \frac{60}{13}, \\ a''_1 &= \frac{7603}{1638}, & a''_2 &= \frac{35290}{7673}, & a''_3 &= \frac{1638}{3529} \end{aligned}$$

ou

$$\begin{aligned} a'_1 &= 4.64163 \ 61416 \ 36 \dots, \\ a'_2 &= 4.64158 \ 88465 \ 08 \dots, \\ a'_3 &= 4.64154 \ 15131 \ 77 \dots \end{aligned}$$

On voit avec quelle rapidité les nombres d'un groupe viennent égaux les uns aux autres; en effet

$$\begin{aligned} a'_1 - a'_2 &= 0.02380 \ 95 \dots, \\ a'_2 - a'_3 &= 0.02747 \ 25 \dots, \\ a''_1 - a''_2 &= 0.00004 \ 72951 \ 38 \dots, \\ a''_2 - a''_3 &= 0.00004 \ 73333 \ 31 \dots \end{aligned}$$

La moyenne des valeurs obtenues pour les nombres d'un groupe, déduits du premier, est

$$a''_1 = 4.64158 \ 88337 \ 74 \dots$$

Nous verrons plus tard que la différence  $a''_1 - a''_2$  est 0.00000 00003. La limite est ici

$$\sqrt[3]{100} = 4.64158 \ 88336 \ 12769 \dots$$

Deuxième exemple.  $k = 4$ .

$$\begin{aligned} a_1 &= 3, & a_2 &= 2, & a_3 &= 2, \\ a'_1 &= \frac{9}{4}, & a'_2 &= \frac{20}{9}, & a'_3 &= \frac{11}{5}, \\ a''_1 &= \frac{17531}{7920}, & a''_2 &= \frac{116410}{52593}, & a''_3 &= \frac{128826}{58205}, \end{aligned}$$

et

$$a'_1 - a'_2 = 0.02777 \ 78 \dots,$$

$$a'_2 - a'_3 = 0.02222 \ 22 \dots,$$

$$a'_3 - a'_4 = 0.01118 \ 18 \dots,$$

$$a''_1 - a''_2 = 0.00009 \ 76697 \ 0 \dots,$$

$$a''_1 - a''_3 = 0.00009 \ 74240 \ 1 \dots,$$

$$a''_3 - a''_4 = 0.00009 \ 71786 \ 0 \dots$$

Des valeurs de  $a'_1$ , de  $a'_2$ , de  $a'_3$  et de  $a'_4$  on tire

$$a'''_1 = 2.21336 \ 38420 \ 8 \dots$$

La limite est ici

$$\sqrt[4]{24} = 2.21336 \ 38394 \ 007 \dots$$

5. Dans les deux exemples donnés on voit que non seulement les différences successives des nombres d'un même groupe telles que

$$a'_1 - a'_2, a'_2 - a'_3, \dots$$

$$a''_1 - a''_2, a''_2 - a''_3, \dots$$

deviennent de plus en plus petites lorsqu'on passe aux groupes suivants, mais aussi que les différences appartenant à un même groupe tendent de plus en plus vers une même valeur.

En effet, on peut énoncer le théorème suivant.

Pour  $n = \infty$  le quotient de deux quelconques des  $(k - 1)$  différences

$$\frac{a_p^{(n)}}{a_{p+1}^{(n)}} - \frac{a_p^{(n)}}{a_{p+1}^{(n)}} \\ (p = 1, 2, 3, \dots, k - 1)$$

tend vers la limite 1.

Parmi les différentes preuves de cette propriété que j'ai trouvées la suivante est de beaucoup la plus simple.

6. Je pose

$$a = a - x$$



de sorte qu'il est impossible que deux des nombres aient la même valeur. Soit encore

$$(9) \quad \begin{cases} f(x) = (x - x_1)(x - x_2) \dots (x - x_k), \\ f(x) = N_0 x^k - \frac{k}{1} N_1 x^{k-1} + \frac{k(k-1)}{1.2} N_2 x^{k-2} - \dots \end{cases}$$

les nombres  $N_0, N_1, \dots, N_k$  sont donc formés à l'aide de  $x_1, x_2, \dots, x_k$  de la même manière que les nombres  $a_1, a_2, \dots, a_k$  ont été formés à l'aide des grandeurs  $a_1, a_2, \dots, a_k$ . Cette ambiguïté ne peut résulter du fait que  $f(x)$  a ici dans la première signification que dans le n° 2. On se convaincra aisément que les nombres  $M_0, M_1, \dots, M_k$  peuvent être exprimés de la même manière à l'aide de la fonction  $f(x)$  et de ses dérivées :

$$(10) \quad \left. \begin{aligned} M_k &= f(a), \\ k M_{k-1} &= f'(a), \\ k(k-1) M_{k-2} &= f''(a), \\ &\dots \dots \dots \\ k(k-1) \dots 3.2 M_1 &= f^{(k-1)}(a), \\ k(k-1) \dots 3.2.1 M_0 &= f^{(k)}(a) \end{aligned} \right\}$$

Il s'ensuit que

$$(11) \quad \dots \dots \dots a'_p = \frac{p f^{(k-p)}(a)}{f^{(k-p+1)}(a)},$$

$$(p = 1, 2, 3, \dots, k)$$

où il faut prendre  $f^0(a) = f(a)$ .

Au lieu de l'équation (11) on peut écrire

$$(12) \quad a'_p = \frac{N_0 a^p - \frac{p}{1} N_1 a^{p-1} + \frac{p(p-1)}{1.2} N_2 a^{p-2} - \dots}{N_0 a^{p-1} - \frac{(p-1)}{1} N_1 a^{p-2} + \frac{(p-1)(p-2)}{1.2} N_2 a^{p-3} - \dots}$$

En développant la formule du second membre en puissances descendantes de  $a$ , on trouve pour les premiers

ces racines sont par hypothèse rangées suivant leur ordre de grandeur, de sorte que

$$y_1 < y_2 < \dots < y_p.$$

Appelons de même  $z_1, z_2, \dots, z_{p-1}$ , grandeurs qui satisfont aux inégalités  $z_1 < z_2 < \dots < z_{p-1}$ , les racines réelles et inégales de l'équation  $f^{(k-p+1)}(x) = 0$ ; de sorte que  $z_1$  est située entre  $y_1$  et  $y_2$ ,  $z_2$  entre  $y_2$  et  $y_3$ ... et enfin  $z_{p-1}$  entre  $y_{p-1}$  et  $y_p$ . Il faut supposer  $p > 1$ . On a alors suivant l'équation (11)

$$a'_p = \frac{(a - y_1)(a - y_2) \dots (a - y_p)}{(a - z_1)(a - z_2) \dots (a - z_{p-1})},$$

et, si l'on exécute la division et qu'on partage le quotient en fractions simples, on aura suivant l'équation (13)

$$(14) \quad \dots \quad a'_p = a - N_1 + \sum_{k=1}^{p-1} \frac{A_k}{a - z_k},$$

où

$$(15) \quad A_k = \frac{(z_k - y_1)(z_k - y_2) \dots (z_k - y_p)}{(z_k - z_1) \dots (z_k - z_{k-1})(z_k - z_{k+1}) \dots (z_k - z_{p-1})}.$$

Dans le numérateur de cette fraction qui représente  $A_k$  les facteurs

$$(z_k - y_1)(z_k - y_2) \dots (z_k - y_k)$$

sont tous positifs; les autres  $(p - k)$  facteurs au contraire, c. à. d. les facteurs

$$z_k - y_{k+1}, z_k - y_{k+2}, \dots, z_k - y_p$$

sont tous négatifs.

Les facteurs négatifs du dénominateur de l'expression  $A_k$  sont

$$z_k - z_{k+1}, z_k - z_{k+2}, \dots, z_k - z_{p-1};$$

leur nombre est de  $p - k - 1$ . Le nombre des facteurs négatifs du

$$a'_p < a - N_1 + \frac{A_1 + A_2 + \dots + A_{p-1}}{a - z_1}$$

et que

$$a'_p > a - N_1 + \frac{A_1 + A_2 + \dots + A_{p-1}}{a - z_{p-1}}$$

Or, l'expression  $A_1 + A_2 + \dots + A_{p-1}$  est évidemment de  $\frac{1}{a}$  dans le développement de  $a'_p$  suivant les puissances de  $a$ ; suivant (13) cette expression est  $-(p-1)(N_1^2 - N_0 N_2)$  et l'on a  $a - z_1 < a - x_1 = a_1$ ,  $a - z_{p-1} > a - x_{p-1} = a_k$ , tandis qu'on a aussi, comme cela se voit aisément

Il s'ensuit donc que

$$(16) \quad \dots \quad \left\{ \begin{array}{l} a'_p < a'_1 - \frac{(p-1)(N_1^2 - N_0 N_2)}{a_1}, \\ a'_p > a'_1 - \frac{(p-1)(N_1^2 - N_0 N_2)}{a_k}. \end{array} \right.$$

Pour  $p=1$  il faut évidemment remplacer les signes  $<$  et  $>$  par le signe  $=$ .

7. Pour pouvoir déduire les inégalités (16) nous avons supposé — et c'était une base essentielle de notre raisonnement — que les grandeurs  $A_1, A_2, \dots, A_{p-1}$  sont toutes négatives; cela peut être démontré encore autrement.

Soit

$$g(x) = (x - y_1)(x - y_2) \dots (x - y_p),$$

il s'ensuit évidemment que

$$a'_p = \frac{p g(a)}{g'(a)}$$

et que

$$\frac{g'(x)}{g(x)} = \frac{1}{x - y_1} + \frac{1}{x - y_2} + \dots + \frac{1}{x - y_p}$$

Or, de l'équation  $a'_p = \frac{p g(a)}{g'(a)}$  on peut tirer immédiatement

$$A_k = \frac{p g(z_k)}{g''(z_k)},$$

donc

$$\frac{p}{A_k} = -\frac{1}{(z_k - y_1)^2} - \frac{1}{(z_k - y_2)^2} - \dots - \frac{1}{(z_k - y_p)^2},$$

d'où il suit que  $A_k$  est négatif.

8. Si l'on remplace  $p$  par  $p + 1$  dans l'équation (16), on obtient en combinant les différentes inégalités

$$a'_p - a'_{p+1} < \frac{a_k + p(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2),$$

$$a'_p - a'_{p+1} > \frac{a_1 - p(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2),$$

donc à plus forte raison, attendu que  $p$  est tout au plus égal à  $k - 1$  et que les expressions  $a_1 - a_k$  et  $N_1^2 - N_0 N_2$  sont positives,

$$17) \quad \dots \quad \left\{ \begin{array}{l} a'_p - a'_{p+1} < \frac{a_k + (k-1)(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2), \\ a'_p - a'_{p+1} > \frac{a_1 - (k-1)(a_1 - a_k)}{a_1 a_k} (N_1^2 - N_0 N_2). \end{array} \right.$$

Les seconds membres de ces équations ne contiennent plus le nombre  $p$ .

Tous les développements antérieurs restent les mêmes, si l'on remplace les nombres  $a_1, a_2, \dots, a_k$ , par  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  et en même temps les nombres  $a'_1, a'_2, a'_k$  par  $a_1^{(n+1)}, a_2^{(n+1)}, \dots, a_k^{(n+1)}$ .

Or, comme nous avons déjà prouvé que les nombres  $a_1^{(n)}, a_2^{(n)}, \dots, a_k^{(n)}$  tendent tous pour  $n = \infty$  vers une même limite positive, on peut apparemment toujours donner à  $n$  une grandeur telle que l'expression

grandeurs entre lesquelles est située l'expression

$$\frac{a_p^{(n+1)} - a_{p+1}^{(n+1)}}{a_q^{(n+1)} - a_{q+1}^{(n+1)}}$$

diffère de l'unité aussi peu qu'on le désire.

Nous avons donc démontré ce qui a été avancé au

9. Pour simplifier les formules, je remplacerai  $a_p^{(n)}$  par  $b_p$  et  $a_p^{(n+1)}$  par  $b'_p$ .

On a donc dans ce cas-là

$$b'_1 - b'_k = \frac{b_1 + b_2 + \dots + b_k}{k} - \frac{k}{\frac{1}{b_1} + \frac{1}{b_2} + \dots}$$

ou

$$\begin{aligned} k \left( \frac{1}{b_1} + \frac{1}{b_2} + \dots + \frac{1}{b_k} \right) (b'_1 - b'_k) = & 1 + \frac{b_2}{b_1} + \frac{b_3}{b_1} + \dots \\ & + \frac{b_1}{b_2} + 1 + \frac{b_3}{b_2} + \dots \\ & + \frac{b_1}{b_3} + \frac{b_2}{b_3} + 1 + \dots \\ & \dots \dots \dots \dots \dots \dots \\ & + \frac{b_1}{b_k} + \frac{b_2}{b_k} + \frac{b_3}{b_k} + \dots \end{aligned}$$

Le second membre peut s'écrire

$$= \Sigma \left( \frac{b_p}{b_q} + \frac{b_q}{b_p} - 2 \right) = \Sigma \frac{(b_p - b_q)^2}{b_p b_q},$$

où  $p$  et  $q$  acquièrent successivement toutes les valeurs avec cette condition qu'on aura toujours  $p > q$ .

Si l'on divise les deux membres par  $(b_1 - b_k)^2$  et limite pour  $n = \infty$  on trouve attendu que d'après



si elle est supérieure à  $\pi$  la limite a la valeur

$$-\sqrt{r_1 r_2} e^{\frac{1}{2}(a_1 + a_2)i}.$$

Si l'on pose par exemple

$$a_1 = z, \quad a_2 = \frac{1}{z},$$

la limite sera  $+1$ , lorsque la partie réelle de  $z$  est positive, et  $-1$  lorsque cette partie est négative.

Comme les expressions

$$a_1, a'_1, a''_1, a'''_1 \dots$$

sont toutes ici des fonctions rationnelles de  $z$ , la somme

$$b_1 + b_2 + b_3 + \dots,$$

où

$$b_1 = a_1, \quad b_2 = a'_1 - a_1, \quad b_3 = a''_1 - a'_1, \quad b_4 = a'''_1 - a''_1, \dots$$

est composée d'une infinité de termes qui sont toutes des fonctions rationnelles de  $z$ . Cette somme tend vers une limite pour toutes les valeurs de  $z$  dont la partie réelle n'est pas nulle. La limite est  $+1$  lorsque la partie réelle de  $z$  est positive, et  $-1$  lorsque elle est négative.

Une série de ce genre a été donnée par Weierstrass dans son article fort important *Zur Functionenlehre*, publié dans les *Berichte der Königl. Preuss. Akademie der Wissenschaften*, p. 735.

Peu après Tannery a remarqué qu'on peut former des séries analogues en suivant une méthode fort simple (Consultez son article dans les *Berichte*, 1881, p. 228 et suiv.).

On apercevra aisément que notre série est comprise dans les cas particuliers dans celles que Weierstrass donne dans son article, p. 230. (Il faut y corriger une faute d'impression : au lieu de  $1+x$  il faut mettre  $1-x$ .)

## IX.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, 193—195.)

---

### Over het quadratische rest-karakter van het getal 2.

1. Zij  $p$  een oneven priemgetal. De getallen kleiner dan  $p$ , met uitzondering van  $p-1$ ,

$$1, 2, 3, \dots, p-2$$

kunnen in twee groepen verdeeld worden, al naar gelang ze quadratische resten of niet-resten van  $p$  zijn. De eerste groep

(A) . . . . .  $a, a', a'', \dots$

bevat dan al de resten, de tweede groep

(B) : . . . . .  $b, b', b'', \dots$

alle niet resten, die onder de getallen  $1, 2, 3, \dots, p-2$  voorkomen. Indien dus  $p-1$  of  $-1$  quadratische rest, dan bevat de groep (A) alle resten van  $p$  behalve  $p-1$ , en de groep (B) bestaat uit de gezamenlijke niet-resten van  $p$ . Is daarentegen  $-1$  quadratische niet rest, dan bestaat de groep (A) uit alle resten, de groep (B) uit alle niet-resten met uitzondering van  $p-1$ . In het eerste geval beva

dus de groep (A)  $\frac{p-3}{2}$ , de groep (B)  $\frac{p-1}{2}$  getallen, in het tweed

geval bevat (A)  $\frac{p-1}{2}$ , (B)  $\frac{p-3}{2}$  getallen.



De getallen van een paar zijn altijd ongelijk; we volgen  $b^2 \equiv 1$ , dus  $b = 1$  of  $b = p - 1$ , maar het  $p$  rest nooit in de groep (B) voor, terwijl  $p - 1$  nooit in (B) voorkomt.

Is dus het geheele aantal  $\frac{p-1}{2}$  der niet-resten van den vorm  $4n + 1$ , dan bevat (B) alle niet-resten is dus rest van  $p$ . Is daarentegen  $\frac{p-1}{2}$  oneven,  $p = 4n + 3$ , dan is noodzakelijk  $-1$  niet-rest van  $p$ .

Te gelijk volgt nu:

voor  $p = 4n + 1$ : (A) bevat alle resten behalve  $-1$ ; aantal der getallen (A) is  $2n - 1$ ; (B) bevat alle resten; aantal is  $2n$ ;

en voor  $p = 4n + 3$ : (A) bevat alle resten; hun aantal is  $2n$ ; (B) bevat alle niet-resten behalve de niet-rest  $p - 1$ ; aantal der getallen (B) is  $2n$ .

2. Door bij alle getallen  $a, a', a'', \dots, b, b', b'', \dots$  te tellen, ontstaan de groepen van getallen

(A') . . . . .  $a + 1, a' + 1, a'' + 1, \dots$

(B') . . . . .  $b + 1, b' + 1, b'' + 1, \dots$ ,

die te zamen alle getallen

$$2, 3, 4, \dots, p - 1$$

vormen; zoodat in (A') en (B') te zamen voorkomen  $\frac{p-3}{2}$  resten en nog  $\frac{p-3}{2}$  resten van  $p$ , namelijk alle resten van  $p$ .

Het aantal der getallen (B') is even, en onder de getallen komen evenveel resten als niet-resten van  $p$  voor.

In verband met het voorgaande volgt, dat voor  $p = 4n + 1$  groep (B') bestaat uit

$$\frac{p-1}{4} = n \text{ resten en uit } \frac{p-1}{4} = n \text{ niet-resten,}$$

en derhalve de groep (A') uit

$$\frac{p-5}{4} = n-1 \text{ resten en uit } \frac{p-1}{4} = n \text{ niet-resten.}$$

Is echter  $p = 4n + 3$ , dan bevat de groep (B')

$$\frac{p-3}{4} = n \text{ resten en } \frac{p-3}{4} = n \text{ niet-resten,}$$

derhalve bevat de groep (A')

$$\frac{p-3}{4} = n \text{ resten en } \frac{p+1}{4} = n+1 \text{ niet-resten.}$$

3. Het quadratische rest-karakter van 2 kan nu als volgt bepaald worden. De gevallen  $p = 4n + 1$ ,  $p = 4n + 3$  moeten afzonderlijk behandeld worden.

I.  $p = 4n + 1$ .

In dit geval bevat (B) alle niet-resten van  $p$ , dus heeft men

$$(x-b)(x-b')(x-b'') \dots \equiv x^{\frac{p-1}{2}} + 1 \pmod{p}.$$

Stelt men hierin  $x = -1$  dan volgt

$$(b+1)(b'+1)(b''+1) \dots \equiv 2 \pmod{p}.$$

Maar volgens  $n^0 2$  komen  $n$  niet-resten voor onder de  $2n$  getallen  $b+1, b'+1, \dots$ , terwijl de overige resten zijn.

II.  $p = 4n + 3$ .

In dit geval bevat (A) alle resten van  $p$ , dus heeft

$$(x - a)(x - a')(x - a'') \dots \equiv x^{\frac{p-1}{2}} - 1 \quad (\text{mod } p)$$

Stelt men hierin  $x = -1$ , dan volgt

$$(a + 1)(a' + 1)(a'' + 1) \dots \equiv 2 \quad (\text{mod } p)$$

Maar volgens n<sup>o</sup> 2 komen  $n + 1$  niet-resten voor op de getallen  $a + 1, a' + 1, \dots$ , terwijl de overige resten

Is dus  $n$  even of

$$p = 8k + 3,$$

dan is 2 niet-rest van  $p$ .

Is  $n$  oneven of

$$p = 8k + 7,$$

dan is 2 rest van  $p$ .

---

## IX.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, 193—195.)  
(traduction)

---

### Le nombre 2 comme résidu quadratique.

1. Supposons que  $p$  représente un nombre premier impair. Les nombres inférieurs à  $p$ , à l'exception de  $p - 1$ , c. à d. les nombres

$$1, 2, 3, \dots, p - 2$$

peuvent être divisés en deux groupes, dont l'un est formé des résidus quadratiques de  $p$ , l'autre des non-résidus de ce nombre. Le premier groupe

(A) . . . . .  $a, a', a'', \dots$

contient donc tous les résidus, le deuxième

(B) . . . . .  $b, b', b'', \dots$

tous les non-résidus compris dans les nombres  $1, 2, 3, \dots, p - 2$ .

Lorsque  $p - 1$  ou  $-1$  est un résidu quadratique, le groupe (A) contient donc tous les résidus de  $p$  excepté  $p - 1$ , et le groupe (B) tous les non-résidus de  $p$ . Mais lorsque  $-1$  est un non-résidu, le groupe (A) se compose de tous les résidus et le groupe B de tous les non-résidus à l'exception de  $p - 1$ . Dans le premier cas le groupe (A)

contient donc  $\frac{p-3}{2}$  et le groupe (B)  $\frac{p-1}{2}$  nombres, dans le deuxième

Les nombres appartenant à un même couple sont premiers entre eux, en effet, de  $b = b'$  on pourrait tirer  $b^2 \equiv b = p - 1$ ; mais le nombre 1 qui est un résidu non-résidu du groupe (B), tandis que le nombre  $p - 1$  ne l'est ni du groupe (A) ni du groupe (B).

Lorsque le nombre total  $\frac{p-1}{2}$  des non-résidus est pair, lorsque  $p$  a la forme  $4n + 1$ , le groupe (B) contient  $\frac{p-1}{2}$  non-résidus de  $p$  et  $-1$  est un résidu de  $p$ . Mais  $\frac{p-1}{2}$  est impair et que  $p$  a la forme  $4n + 3$ , le nombre  $-1$  est nécessairement un non-résidu de  $p$ .

On arrive en même temps aux conclusions suivantes :

a) lorsque  $p = 4n + 1$  : le groupe (A) contient tous les résidus de  $p$  et le résidu  $p - 1$ ; le nombre des termes du groupe (A) est  $2n$ ; le groupe (B) renferme tous les non-résidus; leur nombre est  $2n + 1$ .

b) lorsque  $p = 4n + 3$  : le groupe (A) contient tous les résidus de  $p$ ; leur nombre est  $2n + 1$ ; le groupe (B) contient tous les non-résidus de  $p$  et le non-résidu  $p - 1$ ; le nombre des termes du groupe (B) est  $2n$ .

2. Lorsqu'on ajoute l'unité à tous les nombres  $a, a', a'', \dots$  on obtient les groupes suivants de nombres

(A') . . . . .  $a + 1, a' + 1, a'' + 1, \dots$

(B') . . . . .  $b + 1, b' + 1, b'' + 1, \dots$

Ces deux groupes ensemble contiennent tous les nombres premiers avec  $p$  et

$$2, 3, 4, \dots, p - 1.$$

Il s'ensuit que les groupes (A') et (B') ensemble contiennent  $\frac{p-1}{2}$  non-résidus et encore  $\frac{p-3}{2}$  résidus de  $p$ , c. à d. tous les résidus de  $p$  excepté l'unité.

Le nombre des termes du groupe (B') est pair et

et comme  $b$  est un non-résidu, l'un des nombres  $b + 1$ ,  $b' + 1$  est un résidu, l'autre un non-résidu.

Eu égard à ce qui précède, on peut en déduire que pour  $p = 4n + 1$  le groupe (B') se compose de

$$\frac{p-1}{4} = n \text{ résidus et de } \frac{p-1}{4} = n \text{ non résidus,}$$

et le groupe (A') par conséquent de

$$\frac{p-5}{4} = n \text{ résidus et de } \frac{p-1}{4} = n \text{ non-résidus.}$$

Mais lorsque  $p = 4n + 3$ , le groupe (B') contient

$$\frac{p-3}{4} = n \text{ résidus et } \frac{p-3}{4} = n \text{ non-résidus,}$$

et le groupe (A') par conséquent

$$\frac{p-3}{4} = n \text{ résidus et } \frac{p+1}{4} = n + 1 \text{ non-résidus.}$$

3. Le caractère du nombre 2 comme résidu ou non-résidu peut maintenant être déterminé de la manière suivante. Les cas  $p = 4n + 1$  et  $p = 4n + 3$  doivent être traités séparément.

I.  $p = 4n + 1$ .

Dans ce cas le groupe (B) contient tous les non-résidus de  $p$ , on a donc

$$(x - b)(x - b')(x - b'') \dots \equiv x^{\frac{p-1}{2}} + 1 \pmod{p}.$$

En y substituant à  $x$  la valeur  $-1$ , on trouve

$$(b + 1)(b' + 1)(b'' + 1) \dots \equiv 2 \pmod{p}.$$

Mais lorsque  $n$  est impair, c. à d. lorsque

$$p = 8k + 5,$$

le nombre 2 est non-résidu de  $p$ .

II.  $p = 4n + 3$ .

Dans ce cas le groupe (A) contient tous les résidus

$$(x - a)(x - a')(x - a'') \dots \equiv x^{\frac{p-1}{2}} - 1$$

En y substituant à  $x$  la valeur  $-1$ , on trouve

$$(a + 1)(a' + 1)(a'' + 1) \dots \equiv 2 \quad (\text{mod } p)$$

Mais suivant le n<sup>o</sup> 2 il y a  $n + 1$  non-résidus modulo  $p$ , les nombres  $a + 1, a' + 1, \dots$ , tandis que les autres

Par conséquent lorsque  $n$  est pair, c. à d. lorsque

$$p = 8k + 3,$$

le nombre 2 est non-résidu de  $p$ .

Mais lorsque  $n$  est impair, c. à d. lorsque

$$p = 8k + 7,$$

le nombre 2 est résidu du nombre  $p$ .

---

## X.

Amsterdam, Versl. K. Akad. Wet., 1<sup>e</sup> sect., sér. 2, 17, 1882, 338—417

---

### Bijdrage tot de theorie der derde- en vierde-machtsresten.

Het hoofdtheorem in de theorie der quadraatresten, de zoogenoemde wet van reciprociteit, heeft betrekking op de wederkeerige verhouding van twee oneven priemgetallen, en in eene volledige theorie moet daarom het karakter van het getal 2 als quadraatrest of niet-rest van een ander oneven priemgetal, afzonderlijk bepaald worden. Het getal 2 blijkt hierdoor eene bijzondere plaats onder alle priemgetallen in te nemen.

De theorema's, waardoor het karakter van 2 bepaald wordt, zijn het eerst door Fermat uitgesproken<sup>1)</sup> en door Lagrange<sup>2)</sup> bewezen. Hierbij moet echter vermeld worden dat het bewijs, door Lagrange gegeven, op geheel analoge beschouwingen berust, als die waardoor Euler<sup>3)</sup> reeds vroeger de theorema's bewezen had, die het karakter van 3 als quadraatrest of niet-rest bepalen, en welke insgelijks reeds door Fermat waren uitgesproken. Het is daarom des te meer opmerkelijk, dat Euler steeds te vergeefs getracht heeft, de theorema's omtrent het karakter van 2 te bewijzen (Vergel. Disq. Arithm., art. 120).

Een geheel analoog verschijnsel doet zich voor in de theorie der vierde-machtsresten. Ook hier heeft de algemeene reciprociteitswet betrekking op twee oneven, d. w. z. niet door  $1 + i$  deelbare, priem



rum commentatio secunda, waarin voor het eerst plexe getallen van den vorm  $a + bi$  in de getallentheorie werden, is het biquadratisch karakter van  $1 + i$ . Het daar voorkomende bewijs is zuiver arithmetisch en is wezenlijk op het theorema van art. 71, dat geheel op de hulpstelling, die den grondslag uitmaakt, zoowel als van het vijfde Gaussische bewijs van de reciprocity theorie der quadraatresten. (Theorematis arithmetica nova. Werke, II, p. 1 en Theorematis fundamentalis residuis quadraticis demonstrationes et ampliatioes II, p. 47).

Zooals bekend is, heeft Gauss zijn voornemen in de verhandeling de theorie der vierde-machtsresten tot te brengen door het bewijs te leveren van de algemeene wet, die reeds in de tweede verhandeling over uitgesproken is, niet ten uitvoer gebracht.

De eerste gepubliceerde bewijzen van dit fundamenteel zijn de beide van Eisenstein in het 28<sup>ste</sup> deel van Monatsber. für Mathematik, p. 53 en 223. In het eerste stuk: L. wordt het karakter van  $1 + i$  niet behandeld, wel in der Einfachere Beweis und Verallgemeinerung des Fundamentalsatzes für die biquadratischen Reste. Bij de daar voorkomende van het karakter van  $1 + i$  wordt echter gebruik van vooraf bewezen algemeene reciprociteitswet, wat minder schoon voorkomt, daar de overgang van het algemeene tot het samengestelde toch stellig verlangt het karakter onafhankelijk van het fundamenteeltheorema af te

Hetzelfde geldt in meerdere of mindere mate van methoden, die later bekend gemaakt zijn om de theorie der vierde-machtsresten te behandelen, en voortgezet in de

Geheel analoge opmerkingen zijn te maken omtrent de theorie der derde-machtsresten. Het eerste gepubliceerde bewijs van de door Jacobi uitgesproken wet van reciprociteit in deze theorie is dat van Eisenstein in deel 27 van Crelle's Journal für Mathematik, p. 289. Het afzonderlijk te bepalen karakter van  $1 - \varrho$  (waarin  $\varrho$  een complexe derde-machtswortel der eenheid) is eerst later gegeven door Eisenstein in deel 28, p. 28 e. v. van hetzelfde tijdschrift. Bij deze afleiding wordt weder gebruik gemaakt van de algemeene wet van reciprociteit, en ik zie niet, dat tot dusver eene afleiding van het cubisch karakter van  $1 - \varrho$  gegeven is, waarvan dit niet gezegd kan worden.

Daar het nu toch wenschelijk voorkomt, eene afleiding te bezitten voor het karakter van  $1 + i$  en  $1 - \varrho$ , geheel afgescheiden van de algemeene reciprociteitswetten, zoo is het misschien niet geheel van belang ontbloot om aan te toonen, dat al deze theorema's, die betrekking hebben op de priemgetallen 2,  $1 + i$ ,  $1 - \varrho$  en die tot aanvulling der reciprociteitswetten noodzakelijk zijn, volgens een gelijkblijvende methode bewezen kunnen worden.

Het principe van deze methode bestaat daarin, het priemgetal waarvan het karakter te bepalen is, te vervangen door een congruent product van factoren. Het karakter dezer factoren wordt dan bepaald door beschouwingen, geheel overeenkomstig aan die van Gauss in art. 15—20 van zijne eerste verhandeling over de theorie der vierde-machtsresten (Werke, II, p. 78—87). Gauss beschouwt in deze verhandeling alleen reële getallen, en het doel der verhandeling is de bepaling van het karakter van 2 in deze reële theorie. Het bleef mij echter, dat al de beschouwingen van Gauss bijna onveranderd ook in de theorie der complexe getallen herhaald kunnen worden en de bepaling van het biquadratisch karakter van  $1 + i$  volgt da

van een priemgetal van den vorm  $a + bi$  (waarin  $b$  niet 0 is) om zoo te zeggen mede geheel volbracht; terwijl eene andere methode in het geval, dat de modulus een reëel priemgetal van de vorm  $4n + 3$  is, tot hetzelfde doel gebezigd kan worden. In het laatste geval eene veel eenvoudiger behandeling te vinden (Gauss Werke, II, art 68), heb ik toch gemeend, dat de zelfde wijze als de overige gevallen te moeten behouden. Zoo doende blijkt, dat de gebezigde methode in staat is, alle bekende theorema's af te leiden.

Nadat de bepaling van het biquadratisch karakter gehandeld is, heb ik met behulp van de voorafgaande alle theorema's bewezen, die Gauss door inductie in art. 28 der *Theoria residuorum biquadraticorum* communis opgesteld heeft. Voor zoover mij bekend, zijn deze theorema's voor het eerst bewezen <sup>1)</sup>. Dit bewijs steunt geheel op de theorie der complexe getallen, welke theorie hier dus geheel voldoende dient, daar de theorema's zelf alleen betrekking hebben op reële getallen. Behalve de reciprociteitswet in de theorie der resten, waren voor het volledig bewijs nog de bescijning van art. 19 en 20 noodzakelijk.

Ik zal nu beginnen met de afleiding van het karakter van de theorie der

#### QUADRAATRESTEN.

1. Zij  $p$  een oneven priemgetal, de getallen

$$1, 2, 3, \dots, p-1$$

zullen dan in twee groepen verdeeld worden. Tot

$$A \qquad \alpha, \alpha', \alpha'', \dots$$

worden gerekend alle quadratresten, tot de twee

staat uit  $\frac{p-1}{2}$  volgens den modulus  $p$  incongruente getallen, en men ziet gemakkelijk, dat de beide congruenties:

$$\begin{aligned} (x-a)(x-a')(x-a'') \dots &\equiv x^{\frac{p-1}{2}} - 1 \\ (x-\beta)(x-\beta')(x-\beta'') \dots &\equiv x^{\frac{p-1}{2}} + 1 \end{aligned} \pmod{p}$$

identieke congruenties zijn, want zij zijn van lageren graad dan de  $\left(\frac{p-1}{2}\right)^{\text{den}}$  en bezitten beide blijkbaar  $\frac{p-1}{2}$  wortels, namelijk de eerste de wortels  $x=a, x=a', x=a'', \dots$ , de tweede de wortels  $x=\beta, x=\beta', x=\beta'', \dots$ .

Door bij de getallen van A en B de eenheid op te tellen ontstaat de volgende beide groepen getallen:

$$\begin{array}{ll} A' & \alpha + 1, \alpha' + 1, \alpha'' + 1, \dots \\ B' & \beta + 1, \beta' + 1, \beta'' + 1, \dots \end{array}$$

De aantallen getallen van de groep A', die in A en B voorkomen noem ik nu respectievelijk (0.0), (0.1), en de aantallen getallen van B', die in A en B voorkomen, respectievelijk (1.0), (1.1).

Deze vier getallen kunnen in het volgende schema S vereenigd worden:

$$\begin{array}{cc} (0.0) & (0.1) \\ (1.0) & (1.1) \end{array}$$

Daar de priemgetallen van de vormen  $p=4n+1$  en  $p=4n+3$  zich verschillend gedragen, moeten deze beide gevallen afzonderlijk behandeld worden. Ik begin met het eerste.

2. Voor  $p=4n+1$  is  $-1$  kwadraatrest, zoodat de getallen  $a$  en  $p-a$  tegelijkertijd in A voorkomen. Evenzoo komen de getallen  $\beta$  en  $p-\beta$  gelijktijdig in B voor.

Nu is (0.0) blijkbaar gelijk aan het aantal oplossingen van de con-

Op gelijke wijze omtrent de aantallen (0.0), (1.0), (1.1) blijkt, dat het

teeken	voorstelt het aantal oplossingen van
(0.0)	$\alpha + \alpha' + 1 \equiv 0$
(0.1)	$\alpha + \beta + 1 \equiv 0$
(1.0)	$\beta + \alpha + 1 \equiv 0$
(1.1)	$\beta + \beta' + 1 \equiv 0$

(mod  $p$ )

Men ziet hieruit onmiddellijk, dat

$$(0.1) = (1.0)$$

is; eene tweede betrekking tusschen de getallen van de groep A. Men kan nu overgaan tot de volgende beschouwing. Bij elk getal  $\beta$  van de groep A behoort één bepaald getal van die zelfde groep  $\beta''$ , zoodat

$$\beta \beta'' \equiv 1 \pmod{p}$$

en tevens is dan  $\beta \beta''$  congruent met een getal  $\alpha$  van de groep A.

Door vermenigvuldiging van de congruentie

$$\beta + \beta' + 1 \equiv 0$$

met  $\beta''$  volgt dus

$$1 + \alpha + \beta'' \equiv 0$$

en door deze laatste congruentie met  $\beta$  te vermenigvuldigen, krijgt men de eerste terug. Hieruit valt onmiddellijk af, dat (1.1) = (0.1) is, zoodat het schema S dezen voor

 $h \ j$  $j \ j$ 

Nu komt in de groep A het getal  $p-1$  dus in A welk laatste getal noch in A noch in B voorkomt. De getallen van A' en B' echter komen, zooals evident is, in B voor.

Hieruit volgt

$$h + i + p - 1 = 1$$

De identieke congruentie

$$(x - \beta)(x - \beta')(x - \beta'') \dots \equiv x^{\frac{p-1}{2}} + 1 \pmod{p}$$

geeft nu voor  $x = -1$ , daar  $\frac{p-1}{2}$  even is

$$(\beta + 1)(\beta' + 1)(\beta'' + 1) \dots \equiv 2 \pmod{p}.$$

Het aantal niet-resten onder de getallen  $\beta + 1, \beta' + 1, \beta'' + 1, \dots$  is nu  $(1.1) = j = \frac{p-1}{4}$ .

Is dus  $j$  even of

$$p = 8n + 1,$$

dan is 2 quadraatrest van  $p$ .

Is daarentegen  $j$  oneven of

$$p = 8n + 5,$$

dan is 2 niet-rest van  $p$ .

3. Voor  $p = 4n + 3$  is  $-1$  niet-rest, en de groep B komt overeen met de groep getallen  $p - \alpha, p - \alpha', p - \alpha'', \dots$

Het teeken (0.0) stelt nu voor het aantal oplossingen van de congruentie  $\alpha + 1 \equiv \alpha' \pmod{p}$ , of ook daar  $\alpha' = p - \beta$  is, het aantal oplossingen van  $\alpha + \beta + 1 \equiv 0$ .

Op deze wijze blijkt, dat het

teeken	voorstelt het aantal oplossingen van
(0.0)	$\alpha + \beta + 1 \equiv 0$
(0.1)	$\alpha + \alpha' + 1 \equiv 0 \pmod{p},$
(1.0)	$\beta + \beta' + 1 \equiv 0$
(1.1)	$\beta + \alpha + 1 \equiv 0$

derhalve is  $(0.0) = (1.1)$ . Is verder weder  $\beta\beta'' \equiv 1, \beta'\beta'' \equiv \alpha$ , dan volgt uit  $\beta + \beta' + 1 \equiv 0$  door vermenigvuldiging met  $\beta''$

overigens alle getallen van  $A'$  en  $B'$  òf in  $A$  òf in  $B$  zoo volgt

$$h + j = \frac{p-1}{2},$$

$$2h = \frac{p-1}{2} - 1,$$

dus

$$h = \frac{p-3}{4}, \quad j = \frac{p+1}{4}.$$

Uit de congruentie

$$(x-a)(x-a')(x-a'') \dots \equiv x^{\frac{p-1}{2}} - 1$$

volgt voor  $x = -1$  daar  $\frac{p-1}{2}$  oneven is,

$$(a+1)(a'+1)(a''+1) \dots \equiv 2 \quad (\text{mod } p)$$

en het aantal niet-resten onder de getallen  $a+1, a'+1, \dots$

$$\text{dus } (0.1) = j = \frac{p-1}{4}.$$

Is dus  $j$  even of

$$p = 8n + 7,$$

dan is 2 quadraatrest van  $p$ .

Is daarentegen  $j$  oneven of

$$p = 8n + 3,$$

dan is 2 niet-rest van  $p$ .

Nadat hiermede dus het karakter van 2 als quadraatrest ten opzichte van een willekeurig oneven priemgetal  $p$  ga ik er toe over het overeenkomstige te ontwikkelen.

#### VIERDE-MACHTSRESTEN.

4. Het oneven (d. w. z. niet door  $1+i$  deelbaar) getal  $m = a + bi$  zal steeds primair, in den zin van Gauss worden, zoodat  $a-1$  en  $b$  volgens den modulus 4

ten tweede uit de complexe priemfactoren van de reële priemgetallen van den vorm  $4n+1$ . Deze complexe priemgetallen zijn van den vorm  $a+bi$ , waarin  $b$  niet gelijk nul is, en worden door vermenigvuldiging met ééne bepaalde der vier eenheden  $1, i, -1, -i$  primair. Zij kunnen verder in twee soorten onderscheiden worden al naar gelang, wanneer  $a+bi$  primair is,  $a-1$  en  $b$  beide door  $4$  deelbaar, of beide het dubbel van een oneven getal zijn.

Ik onderscheid hierna deze drie klassen van primaire priemgetallen

I. De reële priemgetallen  $q$  van den vorm  $4r+3$ , negatief genomen.

II. De complexe priemgetallen van den vorm  $4r+1+4si$ .

III. De complexe priemgetallen van den vorm  $4r+3+(4s+2)i$ .

Het priemgetal (in de complexe theorie) zal steeds door  $M$  aangeduid worden, de norm van  $M$  door  $\mu$ . Verder zal steeds  $p$  een reël (positief) priemgetal van den vorm  $4r+1$ ,  $q$  een reël (negatief) priemgetal van den vorm  $4r+3$  voorstellen. De priemgetallen van de eerste soort zijn dus  $M=-q$ ,  $\mu=q^2$ , voor de tweede en derde soort is  $\mu=p$ .

Ik merk nog op, dat voor de beide soorten I en II de norm  $\mu$  van den vorm  $8r+1$ , en voor III van den vorm  $8r+5$  is. Deze omstandigheid maakt, dat de beide eerste soorten van priemgetallen tot op zekere hoogte gemeenschappelijk behandeld kunnen worden.

De beschouwingen van het volgende art. 5 gelden nog gelijkelijk voor de drie klassen van priemgetallen.

5. Zij dan  $M$  het priemgetal,  $\mu$  de norm. Een volledig systeem van incongruente, en niet door den modulus  $M$  deelbare getallen bestaat uit  $\mu-1$  getallen, welke volgens hun biquadratisch karakter

in  $\mu-1$  getallen bevattende



Tot de eerste klasse A worden gebracht alle ge-  
het biquadratisch karakter 0, tot de groepen B  
met het biquadratisch karakter 1, 2, 3.

Ten overvloede zij gezegd, dat hier het biqua-  
in den zin van Gauss genomen wordt, zoodat de  
klassen gekarakteriseerd zijn door de congruentie

$$a^{\frac{\mu-1}{4}} \equiv 1, \beta^{\frac{\mu-1}{4}} \equiv i, \gamma^{\frac{\mu-1}{4}} \equiv -1, \delta^{\frac{\mu-1}{4}} \equiv -i$$

Ik zal mij echter, voor het gemak, eveneens v-  
ingevoerde symbool bedienen, en dus kunnen sch

$$\left(\left(\frac{a}{M}\right)\right) = 1, \left(\left(\frac{\beta}{M}\right)\right) = i, \left(\left(\frac{\gamma}{M}\right)\right) = -1, \left(\left(\frac{\delta}{M}\right)\right) = -i$$

Eindelijk zij eens vooral opgemerkt, dat in he-  
gruenties betrekking zullen hebben op den priem-  
niet uitdrukkelijk een andere modulus is aangege-

Ik laat hier een voorbeeld volgen van de ver-  
(mod M), met uitzondering van de rest 0, in de vier  
voor elk der drie soorten van priemgetallen, d-  
scheiden werden.

			$M = -7,$	$\mu = 49.$
A	1,	-2,	-3,	-1,
	$3i,$	$i,$	$-2i,$	$-3i,$
B	$1 - 2i,$	$-2 - 3i,$	$-3 - i,$	$-1 + 2i,$
	$-1 + 3i,$	$2 + i,$	$3 - 2i,$	$1 - 3i,$
C	$-3 + 3i,$	$-1 + i,$	$2 - 2i,$	$3 - 3i,$
	$-2 - 2i,$	$-3 - 3i,$	$-1 - i,$	$2 + 2i,$
D	$3 + 2i,$	$1 + 3i,$	$-2 + i,$	$-3 - 2i,$
	$1 + 2i,$	$-2 + 3i,$	$-3 + i,$	$-1 + 2i,$
			$M = -3 - 8i,$	$\mu = 73.$

	$4i,$	$4 + 3i,$	$4 - i,$	$-4i,$	$-4 - 3i,$	$-4 +$
C	$-3 + i,$	$i,$	$3,$	$3 - i,$	$-i,$	$-3,$
	$2i,$	$-2 + 3i,$	$-2 + i,$	$-2i,$	$2 - 3i,$	$2 -$
	$-3 - i,$	$2 - 2i,$	$-3 + 2i,$	$3 + i,$	$-2 + 2i,$	$3 - 2$
D	$-4 - i,$	$2 + i,$	$-2 + 5i,$	$4 + i,$	$-2 - i,$	$2 - 5$
	$4 + 2i,$	$1 - i,$	$-3 - 3i,$	$-4 - 2i,$	$-1 + i,$	$3 + 3$

$$M = -5 + 6i, \quad \mu = 61.$$

	$1,$	$-3,$	$-2 + i,$	$1 + 3i,$	$-2 + 2$
A	$-4,$	$1 + i,$	$3 + 2i,$	$-3 - i,$	$3 - 2$
	$-1 - 4i,$	$2 + i,$	$2i,$	$-5,$	$4 +$
	$1 - i,$	$2 - 3i,$	$-1 + 3i,$	$-2 - 3i,$	$4$
B	$1 - 2i,$	$2,$	$5i,$	$1 - 4i,$	$-4 +$
	$1 + 2i,$	$3 - i,$	$2 + 2i,$	$-i,$	$3$
	$-2i,$	$5,$	$-4 - i,$	$1 + 4i,$	$-2 -$
C	$-1 - 3i,$	$2 - 2i,$	$-1,$	$3,$	$2 -$
	$3 + i,$	$-3 + 2i,$	$4,$	$-1 - i,$	$-3 - 2$
	$-2 - 2i,$	$i,$	$-3i,$	$-1 - 2i,$	$-3 +$
D	$2 + 3i,$	$-4i,$	$-1 + i,$	$-2 + 3i,$	$1 - 3$
	$-1 + 4i,$	$4 - i,$	$-1 + 2i,$	$-2,$	$-5$

Evenals in art. 1 overtuigt men zich onmiddellijk, dat de nu volgende congruenties identiek zijn :

$$\begin{aligned}
 (x - \alpha)(x - \alpha')(x - \alpha'') \dots &\equiv x^{\frac{\mu-1}{4}} - 1 \\
 (x - \beta)(x - \beta')(x - \beta'') \dots &\equiv x^{\frac{\mu-1}{4}} - i \\
 (x - \gamma)(x - \gamma')(x - \gamma'') \dots &\equiv x^{\frac{\mu-1}{4}} + 1 \\
 (x - \delta)(x - \delta')(x - \delta'') \dots &\equiv x^{\frac{\mu-1}{4}} + i
 \end{aligned} \quad (\text{mod } M),$$

waaruit voor  $x = -1$  volgt, de gevallen  $\mu = 8n + 1$  en  $\mu = 8n +$

6. Laten wij nu verder de nieuwe groepen van  $A'$  en  $D'$  beschouwen, die ontstaan door bij de getallen  $D$  de eenheid op te tellen:

$$\begin{array}{ll} A' & \alpha + 1, \alpha' + 1, \alpha'' + 1, \dots \\ B' & \beta + 1, \beta' + 1, \beta'' + 1, \dots \\ C' & \gamma + 1, \gamma' + 1, \gamma'' + 1, \dots \\ D' & \delta + 1, \delta' + 1, \delta'' + 1, \dots \end{array}$$

en noemen wij nu de aantallen getallen van  $A'$ , met getallen van  $A, B, C, D$ , respectievelijk  
 $(0.0), (0.1), (0.2), (0.3);$   
 de aantallen getallen van  $B'$ , die congruent zijn met  $A, B, C, D$ , respectievelijk

$$(1.0), (1.1), (1.2), (1.3).$$

Evenzoo hebben de getallen

$$(2.0), (2.1), (2.2), (2.3)$$

betrekking op de groep  $C'$  en de getallen

$$(3.0), (3.1), (3.2), (3.3)$$

op de groep  $D'$ .

Men kan al deze 16 getallen  $(0.0), (0.1)$ , enz. volgende quadratische schema  $S$ :

$$\begin{array}{cccc} (0.0) & (0.1) & (0.2) & (0.3) \\ (1.0) & (1.1) & (1.2) & (1.3) \\ (2.0) & (2.1) & (2.2) & (2.3) \\ (3.0) & (3.1) & (3.2) & (3.3) \end{array}$$

en voor de voorbeelden in art. 5 gegeven, verkrijgt men

$$M = -7, \mu = 49. \quad M = -3 - 8i, \mu = 73. \quad M = -1 - 2i, \mu = 13.$$

$$\begin{array}{cccc} S & 5 & 2 & 2 & 2 & 5 & 6 & 4 & 2 \\ & 2 & 2 & 4 & 4 & 6 & 2 & 5 & 5 \\ & 2 & 4 & 2 & 4 & 4 & 5 & 4 & 5 \\ & 2 & 4 & 4 & 2 & 2 & 5 & 5 & 6 \end{array}$$

Volgens de congruenties van het voorgaande a

die respectievelijk tot de klassen A, B, C, D behooren, bedragen (3.0), (3.1), (3.2), (3.3), zoo volgt onmiddellijk, dat voor  $\mu = 8n + 1$  het biquadratisch karakter van  $1 + i$  volgens den modulus 4 congruen al zijn met

$$(3.1) + 2(3.2) + 3(3.3)$$

en evenzoo voor het geval  $\mu = 8n + 5$  met

$$(1.1) + 2(1.2) + 3(1.3).$$

Zoodra dus de getallen (0.0), (0.1), enz bepaald zijn, is hiermede ook onmiddellijk het biquadratisch karakter van  $1 + i$  bekend.

Het komt er dus nu op aan, de getallen van het schema S onmiddellijk uit het gegeven primaire priemgetal  $M = a + bi$  af te leiden. De hiertoe noodige beschouwingen zijn wezenlijk dezelfde als die van Gauss in art. 16—20 der *Theoria residuorum biquadraticorum commentatio prima*

Gauss handelt daar over de theorie der reële getallen, maar het blijkt gemakkelijk, dat het daar gegevene in zeer nauw verband staat met het vraagstuk, dat ons hier bezig houdt.

Om de geheele ontwikkeling voor oogen te hebben, zal het noodig zijn hier de argumentatie van Gauss met de geringe noodige wijzigingen te laten volgen.

Hierbij valt ook nog op te merken dat, voor een priemgetal  $M = -q$  tot de eerste klasse van art. 4 behorende, er in de reële theorie van Gauss niets analoogs bestaat, met wat hier in de theorie der geheele complexe getallen ontwikkeld zal worden.

Voor de verdere beschouwingen is het in de eerste plaats noodig de beide gevallen, dat de norm  $\mu$  van den vorm  $8n + 1$  of van de vorm  $8n + 5$  is, afzonderlijk te behandelen. Ik zal met het eerstgenoemde geval, waarin dus het priemgetal  $M$  tot een der beide eerste klassen van art. 4 behoort, beginnen.

elkander vervangen kunnen, als gelijk te beschouwen, het gemak van deze zienswijze gebruik maken, eenige onduidelijkheid zal kunnen ontstaan

Daar dus het biquadratisch karakter van — volgt, dat wanneer  $\alpha, \beta, \gamma, \delta$  respectievelijk tot behooren, ook  $-\alpha, -\beta, -\gamma, -\delta$  in deze zelfde en wel  $-\alpha$  in A,  $-\beta$  in B,  $-\gamma$  in C en  $-\delta$  in

Nu is blijkbaar het getal (0.0) gelijk aan het van de congruentie

$$\alpha + 1 \equiv \alpha' \pmod{M},$$

waarbij  $\alpha$  en  $\alpha'$  op willekeurige wijze uit de gro maar daar bij elk getal  $\alpha'$  een getal  $\alpha'' = p - \alpha'$  aantal oplossingen hetzelfde als dat van de con

$$\alpha + \alpha'' + 1 \equiv 0 \pmod{M},$$

waarin weder  $\alpha$  en  $\alpha''$  uit A te nemen zijn.

Geheel op dezelfde wijze omtrent de getallen ( neerende, overtuigt men zich dat

het teeken      voorstelt het aantal oplossinge

$$(0.0) \quad \alpha + \alpha' + 1 \equiv 0$$

$$(0.1) \quad \alpha + \beta + 1 \equiv 0$$

$$(0.2) \quad \alpha + \gamma + 1 \equiv 0$$

$$(0.3) \quad \alpha + \delta + 1 \equiv 0$$

$$(1.0) \quad \beta + \alpha + 1 \equiv 0$$

$$(1.1) \quad \beta + \beta' + 1 \equiv 0$$

$$(1.2) \quad \beta + \gamma + 1 \equiv 0$$

$$(1.3) \quad \beta + \delta + 1 \equiv 0$$

$$(2.0) \quad \gamma + \alpha + 1 \equiv 0$$

$$(2.1) \quad \gamma + \beta + 1 \equiv 0$$

(m

Hieruit volgen dus onmiddellijk deze zes betrekkingen:

$$\begin{aligned}(0.1) &= (1.0), & (0.2) &= (2.0), & (0.3) &= (3.0), \\ (1.2) &= (2.1), & (1.3) &= (3.1), \\ (2.3) &= (3.2).\end{aligned}$$

Vijf nieuwe betrekkingen tusschen de getallen (0.0), (0.1), enz. verkrijgt men door de volgende beschouwing. Zijn  $\alpha, \beta, \gamma$  getallen van A, B, C en bepaalt men  $x, y, z$  zoodanig dat

$$\alpha x \equiv 1, \beta y \equiv 1, \gamma z \equiv 1 \pmod{M}$$

is, dan behoort blijkbaar  $x$  tot de klasse A,  $y$  tot D,  $z$  tot C, zoodat men kan schrijven

$$\alpha \alpha' \equiv 1, \beta \delta' \equiv 1, \gamma \gamma' \equiv 1.$$

Vermenigvuldigt men nu, terwijl men eene bepaalde oplossing van  $\alpha + \beta + 1 \equiv 0$  beschouwt, deze congruentie met  $\delta$  dan volgt  $\delta' + 1 + \delta \equiv 0$  waarin  $\delta' \equiv \alpha \delta$  tot D behoort. Ongekeerd volgt uit  $\delta' + 1 + \delta \equiv 0$  door vermenigvuldiging met  $\beta$  weder  $\alpha + \beta + 1 \equiv 0$ . Hieruit blijkt dus, dat het aantal oplossingen van de beide congruenties

$$\alpha + \beta + 1 \equiv 0 \text{ en } \delta + \delta' + 1 \equiv 0$$

even groot is, zoodat men heeft (0.1) = (3.3).

Geheel op dezelfde wijze heeft men

$$\begin{aligned}\gamma'(\alpha + \gamma + 1) &\equiv \gamma'' + 1 + \gamma, \\ \beta(\alpha + \delta + 1) &\equiv \beta' + 1 + \beta, \\ \delta(\beta + \gamma + 1) &\equiv 1 + \beta' + \delta, \\ \gamma'(\beta + \gamma + 1) &\equiv \delta + 1 + \gamma',\end{aligned}$$

waaruit men op dezelfde wijze besluit tot

$$(0.2) = (2.2), \quad (0.3) = (1.1), \quad (1.2) = (1.3) = (2.3).$$

Hiermede zijn dus elf betrekkingen tusschen de zestien getallen van het schema S gevonden, en deze getallen worden hierdoor teruggebracht tot vijf verschillende, die door  $h, j, k, l, m$  aangeduid zullen worden. Het schema S neemt nu deze gedaante aan:

$$\begin{array}{cccc} h & j & k & l \\ i & l & m & m \end{array}$$

8. Het getal  $-1$  komt in  $A$  voor, waarmede  $d$  van  $A'$  correspondeert. Dit getal  $0$  van  $A'$  komt in  $A, B, C, D$  voor, maar elk ander getal van  $A'$  komt in één der groepen  $A, B, C$  of  $D$  voor. Daar  $\mu = 8n + 1$  zoo volgt dus

$$(0.0) + (0.1) + (0.2) + (0.3) = 2n - 1.$$

Alle getallen van  $B', C', D'$  komen in één der  $k$  groepen voor, zoodat men heeft

$$(1.0) + (1.1) + (1.2) + (1.3) = 2n,$$

$$(2.0) + (2.1) + (2.2) + (2.3) = 2n,$$

$$(3.0) + (3.1) + (3.2) + (3.3) = 2n.$$

Deze vier vergelijkingen herleiden zich tot de volgende vier trekkingen tusschen  $h, j, k, l$  en  $m$

$$h + j + k + l = 2n - 1,$$

$$j + l + 2m = 2n,$$

$$k + m = n.$$

9. Eindelijk wordt nog eene verdere, niet lineaire congruentie tusschen  $h, j, k, l, m$  verkregen door de beschouwing der oplossingen der congruentie

$$\alpha + \beta + \gamma + 1 \equiv 0 \pmod{M},$$

waarin  $\alpha, \beta, \gamma$  op alle mogelijke wijzen uit de  $k$  groepen kiezen zijn.

Neemt men nu vooreerst voor  $\alpha$  achtereenvolgende waarden van  $A$ , dan gebeurt het respectievelijk  $h, j, k, l$  malen in  $A, B, C, D$  behoort en de enkele maal dat  $\alpha + 1$  buiten beschouwing blijven, daar de congruentie in de enkele oplossing toelaat.

Voor elke bepaalde der  $h$  waarden, die  $\alpha + 1 \equiv \alpha_0 \pmod{M}$  is, kan men nog verder  $\beta$  en  $\gamma$  zóó te kiezen, dat

Daar deze redeneering toepasselijk is voor elke der  $h$  waarden die maken, dat  $a+1$  weder tot A behoort, zoo verkrijgt men op deze wijze  $hm$  oplossingen van de congruentie

$$1 + \alpha + \beta + \gamma \equiv 0.$$

Het gebeurt verder  $j$  malen, dat  $a+1$  tot B behoort, en voor elke bepaalde waarde  $a+1 \equiv \beta_0$  heeft de congruentie

$$\beta_0 + \beta + \gamma \equiv 0$$

hetzelfde aantal oplossingen als de congruentie

$$1 + \alpha + \beta' \equiv 0,$$

dus is dit aantal gelijk  $j$ . Het gezegde blijkt onmiddellijk uit

$$\delta_0(\beta_0 + \beta + \gamma) \equiv 1 + \alpha + \beta',$$

wanneer  $\beta_0 \delta_0 \equiv 1$ .

Deze waarden van  $\alpha$ , die  $a+1$  tot B doen behooren, geven dus in het geheel  $jj$  oplossingen van de beschouwde congruentie.

Voor  $a+1 \equiv \gamma_0$ , wat  $k$  malen gebeurt, heeft de congruentie

$$\gamma_0 + \beta + \gamma \equiv 0$$

$k$  oplossingen, want

$$\gamma'_0(\gamma_0 + \beta + \gamma) \equiv 1 + \delta + \alpha.$$

De waarden van  $\alpha$ , die  $a+1$  tot C doen behooren, leveren dus in het geheel  $kl$  oplossingen.

Is eindelijk  $a+1 \equiv \delta_0$ , wat  $l$  malen gebeurt, dan heeft de congruentie

$$\delta_0 + \beta + \gamma \equiv 0$$

wegens

$$\beta_0(\delta_0 + \beta + \gamma) \equiv 1 + \gamma + \delta$$

$lm$  oplossingen, en deze waarden van  $\alpha$  geven dus  $lm$  oplossingen.

Het totale aantal oplossingen van de congruentie



$k, m, k, m$  oplossingen van de gegeven congruentie zijn, zoodat het totale aantal oplossingen bedraagt

$$jk + lm + mk + mm.$$

10. De gelijkstelling van deze beide uitdrukkingen voor het aantal oplossingen van  $a + \beta + \gamma + 1 \equiv 0$  geeft

$$0 = hm + jj + kl - jk - km - mm,$$

en  $h$  elimineerende met behulp van  $h = 2m - k - 1$ , welke waarde gemakkelijk uit de in art. 8 verkregen vergelijkingen tusschen  $h, j, k, l, m$  volgt, komt er

$$0 = (k - m)^2 + jj + kl - jk - kk - m.$$

Volgens de relaties in art. 8 is

$$k = \frac{1}{2}(j + l)$$

en deze waarde in  $jj + kl - jk - kk$  overbrengende, wordt deze uitdrukking gelijk aan  $\frac{1}{4}(l - j)^2$ , zoodat de voorgaande vergelijking, na vermenigvuldiging met 4, overgaat in

$$0 = 4(k - m)^2 + (l - j)^2 - 4m,$$

maar men heeft

$$4m = 2(k + m) - 2(k - m) = 2n - 2(k - m),$$

dus is

$$2n = 4(k - m)^2 + 2(k - m) + (l - j)^2,$$

of wel

$$\mu = 8n + 1 = [4(k - m) + 1]^2 + 4(l - j)^2,$$

en stellende

$$4(k - m) + 1 = A, \quad 2(l - j) = B,$$

vindt men

$$\mu = A^2 + B^2.$$

Hierin is  $A \equiv 1 \pmod{4}$ , en  $B$  even.

Men kan nu met behulp van  $A$  en  $B$  gemakkelijk  $h, j, k, l, m$  uitdrukken en verkrijgt zodoende

$$8h = 4n - 3A - 5,$$

$$8j = 4n + A - 2B - 1,$$

$$8k = 4n + A - 1,$$

$$8l = 4n + A + 2B - 1,$$

$$8m = 4n - A + 1.$$

$8n+1$  had; voor de verdere bepaling van A en B is het evenwel nu noodig, de gevallen I en II van art. 4 afzonderlijk te behandelen

11. Zij dan vooreerst

$$M = -q = -(4r + 3).$$

In dit geval is

$$\mu = M^2 = q^2$$

en dus

$$q^2 = A^2 + B^2;$$

$q$  een priemgetal van den vorm  $4r + 3$  zijnde, weet men dat  $q^2$  op geen andere wijze als som van twee quadraten voorgesteld kan worden, dan door voor de basis van het eene (oneven) kwadraat  $\pm q$ , voor die van het andere kwadraat 0 te nemen; inderdaad waargenomen der getallen A en B gelijk 0 of door  $q$  deelbaar, dan zou men een van 0 verschillend getal  $x$  kunnen bepalen, zoodat

$$Ax \equiv B \pmod{q}.$$

Nu volgt uit  $q^2 = A^2 + B^2$

$$A^2 \equiv -B^2 \pmod{q}$$

en daar men heeft

$$A^2 x^2 \equiv B^2 \pmod{q},$$

zou er volgen

$$x^2 \equiv -1 \pmod{q}.$$

Deze laatste congruentie nu is onmogelijk, omdat  $-1$  quadratisch niet-rest van  $q$  is.

Uit  $q^2 = A^2 + B^2$  volgt dus noodzakelijk

$$A = \pm q, \quad B = 0$$

en daar  $A \equiv 1 \pmod{4}$ , zoo wordt hierdoor nog het teeken van A vast komen bepaald en is

$$A = -q = M.$$

Nadat op deze wijze A en B gevonden zijn, heeft men nu

$$8h = 4n - 3M - 5,$$

$$8j = 4n + M - 1,$$

$$8k = 4n + M - 1,$$

$$8l = 4n + M - 1,$$

$$8m = 4n - M + 1,$$

waarin  $8n + 1 = M^2$ .

Door deze formules wordt dus de afhankelijkheid der getallen van het schema S van het priemgetal M op de eenvoudigste wijze uitgedrukt, voor het geval dat M tot de eerste klasse van art. behoort.

12. Is in de tweede plaats  $M = a + b i$ , waarin  $a - 1 \equiv b \equiv 0 \pmod{4}$  en de norm  $\mu = a^2 + b^2$  een reëel priemgetal, dan is dus

$$\mu = a^2 + b^2 = A^2 + B^2.$$

Nu kan een priemgetal van den vorm  $4k + 1$  slechts op één wijze voorgesteld worden door de som van twee quadraten, en daar  $a$  en  $A$  beide  $\equiv 1 \pmod{4}$  zijn, zoo volgt  $A = a$ ,  $B = \pm b$ .

Het teeken van  $B$  wordt door de volgende beschouwing bepaald waarbij het noodig is deze hulpstelling vooraf te bewijzen:

„Doorloopt  $z$  een volledig restsysteem  $\pmod{M}$  met uitzondering van den door  $M$  deelbaren term, dan is

$$\sum z^t \equiv -1 \quad \text{of} \quad \equiv 0 \pmod{M},$$

al naardat  $t$  door  $\mu - 1$  deelbaar is of niet.”

Het eerste gedeelte is duidelijk, want is  $t$  door  $\mu - 1$  deelbaar, dan is  $z^t \equiv 1$ , dus  $\sum z^t \equiv \mu - 1 \equiv -1 \pmod{M}$ .

Om ook het tweede gedeelte aan te toonen, zij  $g$  een primitieve wortel voor het priemgetal  $M$ , zoodat de waarden, die  $z$  doorloopt, congruent zijn met

$$g^0, g^1, g^2, g^3, \dots, g^{\mu-2}.$$

Hieruit volgt dus

$$\sum z^t \equiv 1 + g^t + g^{2t} + \dots + g^{(\mu-2)t} \pmod{M},$$

of

$$(1 - g^t) \sum z^t \equiv 1 - g^{(\mu-1)t} \equiv 0 \pmod{M}.$$

Is nu  $t$  niet door  $\mu - 1$  deelbaar, dan is  $1 - g^t$  niet door  $M$  deelbaar en dus  $\sum z^t \equiv 0$ . w. t. b. w.

van  $z$  betrekking heeft als zooeven,

$$\Sigma (z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1 \pmod{M}.$$

Maar aan den anderen kant vormen de getallen  $z^2$  in hun geheel opeenvolgbaar alle getallen van de groepen A en C te zamen, elk deze getallen tweemaal genomen. Van de getallen

$$z^2 + 1$$

behooren er dus

$$2(0.0) + 2(2.0) \quad \text{tot A,}$$

$$2(0.1) + 2(2.1) \quad \text{tot B,}$$

$$2(0.2) + 2(2.2) \quad \text{tot C,}$$

$$2(0.3) + 2(2.3) \quad \text{tot D,}$$

en daar de  $\left(\frac{\mu-1}{4}\right)^{\text{de}}$  machten der getallen van A, B, C, D respectievelijk congruent zijn met 1,  $i$ ,  $-1$ ,  $-i$ , zoo volgt dus

$$\begin{aligned} \Sigma (z^2 + 1)^{\frac{\mu-1}{4}} &\equiv 2 [(0.0) + (2.0) - (0.2) - (2.2)] + \\ &\quad + 2i [(0.1) + (2.1) - (0.3) - (2.3)] \\ &\equiv 2(h - k) + 2i(j - l), \end{aligned}$$

of de waarden van art. 10 invoerende, daar  $A = a$  is,

$$\Sigma (z^2 + 1)^{\frac{\mu-1}{4}} \equiv -a - 1 - Bi.$$

Uit de vergelijking met het eerste resultaat

$$\Sigma (z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1$$

volgt nu

$$a + Bi \equiv 0 \pmod{M = a + bi},$$

plus

$$B = b.$$

Hierdoor gaan dan ten slotte de waarden van  $h, j, k, l, m$  van art. 10 over in

$$8h = 4n - 3a - 5,$$

$$8j = 4n + a - 2b - 1,$$

$$8k = 4n + a - 1,$$

$$8l = 4n + a + 2b - 1,$$

$$8m = 4n - a + 1,$$

waarin dus  $8n + 1 = a^2 + b^2$  de norm is van het priemgetal  $M$ .

gehandeld zijn, moet nu het geval  $\mu = 8n + 5$  beschouwd worden

Daar dan  $\frac{\mu-1}{4}$  oneven is, zoo behoort  $-1$  tot de groep C, evenzooals gemakkelijk te zien is, behooren de getallen

$$p - \alpha, p - \alpha', p - \alpha'', \dots$$

alle tot C, en de getallen

$$p - \beta, p - \beta', p - \beta'', \dots$$

alle tot D.

Met behulp van deze opmerkingen volgt nu zonder moeite, dat

het teeken	voorstelt het aantal oplossingen van	
(0.0)	$\alpha + \gamma + 1 \equiv 0$	
(0.1)	$\alpha + \delta + 1 \equiv 0$	
(0.2)	$\alpha + \alpha' + 1 \equiv 0$	
(0.3)	$\alpha + \beta + 1 \equiv 0$	
(1.0)	$\beta + \gamma + 1 \equiv 0$	
(1.1)	$\beta + \delta + 1 \equiv 0$	
(1.2)	$\beta + \alpha + 1 \equiv 0$	
(1.3)	$\beta + \beta' + 1 \equiv 0$	
(2.0)	$\gamma + \gamma' + 1 \equiv 0$	(mod M),
(2.1)	$\gamma + \delta + 1 \equiv 0$	
(2.2)	$\gamma + \alpha + 1 \equiv 0$	
(2.3)	$\gamma + \beta + 1 \equiv 0$	
(3.0)	$\delta + \gamma + 1 \equiv 0$	
(3.1)	$\delta + \delta' + 1 \equiv 0$	
(3.2)	$\delta + \alpha + 1 \equiv 0$	
(3.3)	$\delta + \beta + 1 \equiv 0,$	

waaruit dan zes betrekkingen voortvloeien

$$\begin{aligned} (0.0) &= (2.2), & (0.1) &= (3.2), & (0.3) &= (1.2), \\ (1.0) &= (2.3), & (1.1) &= (3.3), & & \\ (2.1) &= (3.0). \end{aligned}$$

Daar evenals vroeger  $\alpha \alpha' \equiv \beta \delta \equiv \gamma \gamma' \equiv 1$ , zoo heeft men

$$\begin{aligned} \gamma' (\alpha + \gamma + 1) &\equiv \gamma'' + 1 + \gamma', \\ \beta (\alpha + \delta + 1) &\equiv \beta' + 1 + \beta, \\ \delta (\alpha + \beta + 1) &\equiv \delta' + 1 + \delta, \\ \delta (\beta + \gamma + 1) &\equiv 1 + \beta' + \delta, \\ \gamma' (\beta + \gamma + 1) &\equiv \delta + 1 + \gamma', \end{aligned}$$

$$(0.0) = (2.0), \quad (0.1) = (1.3), \quad (0.3) = (3.1), \\ (1.0) = (1.1) = (2.1).$$

Ten gevolge van deze elf betrekkingen neemt het schema S deze vorm aan

$$\begin{array}{cccc} h & j & k & l \\ m & m & l & j \\ h & m & h & m \\ m & l & j & m. \end{array}$$

Daar  $-1$  in de groep C, dus 0 in C' voorkomt, zoo volgt geheel op dezelfde wijze als in art. 8

$$\begin{aligned} h + j + k + l &= \frac{\mu - 1}{4} = 2n + 1, \\ 2m + l + j &= 2n + 1, \\ h + m &= n. \end{aligned}$$

De beschouwing van het aantal oplossingen der congruentie

$$a + \beta + \gamma + 1 \equiv 0$$

gebeurt eindelijk nog eene vergelijking tusschen  $h, j, k, l, m$  op. Neemt men eerst voor  $a$  alle waarden, die tot A behooren, dan gebeurt het respectievelijk  $h, j, k, l$  malen, dat  $a + 1$  tot de groepen A, B, C, D behoort. En verder vindt men op dezelfde wijze als in art. 9, dat voor elk dezer gevallen de congruentie respectievelijk  $m, l, j, m$  oplossingen heeft, waaruit dus voor het totale aantal oplossingen volgt

$$hm + jl + kj + lm.$$

Neemt men daarentegen eerst voor  $\beta$  alle waarden van B, dan gebeurt het respectievelijk  $m, m, l, j$  malen, dat  $\beta + 1$  tot de groepen A, B, C, D behoort. En verder vindt men, dat voor elk dezer gevallen de congruentie respectievelijk  $h, m, h, m$  oplossingen heeft, zoodat het totale aantal oplossingen ook bedraagt

$$mh + mm + lh + jm.$$

14. De gelijkstelling van de beide uitdrukkingen voor het aantal oplossingen der congruentie

$$a + \beta + \gamma + 1 \equiv 0 \pmod{M}$$

geeft

$$0 = m^2 + lh + jm - jl - kj - lm,$$

of daar  $k = 2m - h$  is, zooals uit de lineaire betrekkingen tusschen  $h, j, k, l, m$  in art. 13 dadelijk volgt,

$$0 = m^2 + lh + hj - jl - jm - lm.$$

Drukt men nu met behulp van  $j + l = 1 + 2h$ ,  $j$  en  $l$  beide uit door hun verschil

$$2j = 1 + 2h + (j - l),$$

$$2l = 1 + 2h + (j - l);$$

dan gaat de voorgaande vergelijking door invoering van deze waarden over in

$$0 = 4m^2 - 4m - 1 + 4h^2 - 8hm + (j - l)^2,$$

of daar

$$4m = 2(h + m) - 2(h - m) = 2n - 2(h - m),$$

komt er

$$0 = 4(h - m)^2 - 2n + 2(h - m) - 1 + (j - l)^2$$

en eindelijk

$$\mu = 8n + 5 = [4(h - m) + 1]^2 + 4(j - l)^2,$$

dus voor

$$A = 4(h - m) + 1, \quad B = 2j - 2l,$$

heeft men

$$\mu = A^2 + B^2.$$

Met behulp van  $A$  en  $B$  kan men nu gemakkelijk  $h, j, k, l, m$  uitdrukken, als volgt

$$8h = 4n + A - 1,$$

$$8j = 4n + A + 2B - 3,$$

$$8k = 4n - 3A + 3,$$

$$8l = 4n + A - 2B + 3,$$

$$8m = 4n - A + 1.$$

Er blijft nog over  $A$  en  $B$  te bepalen. Nu is  $\mu$  als reëel priemgetal van den vorm  $4n + 1$  slechts op één wijze voor te stellen door een som van twee tweedemachten, en daar

$$M = a + bi$$

is, heeft men

$$\mu = a^2 + b^2,$$

waarin

$$A = -a \text{ en } B = \pm b.$$

Om het teeken van  $B$  te bepalen dient eene beschouwing analoog aan die in art. 12.

Men vindt gemakkelijk

$$\Sigma(z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1 \equiv 2(h-k) + 2i(j-l) \pmod{M}.$$

Nu is

$$2(h-k) = A-1, \quad 2(j-l) = B,$$

dus heeft men

$$-1 \equiv A-1 + Bi,$$

$$0 \equiv A + Bi \pmod{M=a+bi}.$$

Daar nu reeds gevonden werd  $A = -a$ , zoo volgt  $B = -b$  en ten slotte is dus

$$\begin{aligned} 8h &= 4n - a - 1, \\ 8j &= 4n - a - 2b + 3, \\ 8k &= 4n + 3a + 3, \\ 8l &= 4n - a + 2b + 3, \\ 8m &= 4n + a + 1. \end{aligned}$$

15. De verkregen resultaten samenstellende, is dus voor  $\mu = 8n + 1$  het schema  $S$  van den vorm

$$\begin{array}{cccc} h & j & k & l \\ j & l & m & m \\ k & m & k & m \\ l & m & m & j \end{array}$$

waarin:

$$\begin{aligned} \text{voor } M = -q \quad 8h &= 4n - 3M - 5, \\ 8j &= 8k = 8l = 4n + M - 1, \\ 8m &= 4n - M + 1. \end{aligned}$$

$$\begin{aligned} \text{voor } M = a + bi \quad 8h &= 4n - 3a - 5, \\ 8j &= 4n + a - 2b - 1, \\ 8k &= 4n + a - 1, \\ 8l &= 4n + a + 2b - 1, \\ 8m &= 4n - a + 1. \end{aligned}$$



$h$	$j$	$k$	$l$
$m$	$m$	$l$	$j$
$h$	$m$	$h$	$m$
$m$	$l$	$j$	$m$

waarin

$$\begin{aligned} 8h &= 4n - a - 1, \\ 8j &= 4n - a - 2b + 3, \\ 8k &= 4n + 3a + 3, \\ 8l &= 4n - a + 2b + 3, \\ 8m &= 4n + a + 1. \end{aligned}$$

Zooals uit deze formules blijkt, correspondeert de verandering van  $b$  in  $-b$  met eene verwisseling van  $j$  en  $l$ , zoowel in het geval  $\mu = 8n + 1$ , als wanneer  $\mu = 8n + 5$  is

Volgens de congruenties van art. 5 is nu voor  $\mu = 8n + 1$  het karakter van  $1 + i$  naar den mod 4 congruent met

$$(3.1) + 2(3.2) + 3(3.3) = 3m + 3j \equiv -m - j$$

en dat van  $1 - i$  congruent met

$$(1.1) + 2(1.2) + 3(1.3) = l + 5m \equiv l + m$$

en dus vindt men voor  $M = -q$

$$\text{Karakter } (1 + i) \equiv -n = -\frac{q^2 - 1}{8},$$

$$\text{Karakter } (1 - i) \equiv n = \frac{q^2 - 1}{8}.$$

Nu zijn  $\frac{q+1}{4}$  en  $\frac{q-3}{4}$  geheele, op elkaar volgende getallen, dus is hun product even, en  $\frac{(q+1)(q-3)}{8}$  door 4 deelbaar, zoodat men heeft

$$\frac{q^2 - 1}{8} \equiv \frac{q^2 - 1}{8} - \frac{(q+1)(q-3)}{8} = \frac{q+1}{4}.$$

Hieruit volgt

$$\left(\left(\frac{1+i}{M}\right)\right) = i^{\frac{M-1}{4}}, \quad \left(\left(\frac{1-i}{M}\right)\right) = i^{\frac{M-1}{4}},$$

en daar  $-1$  biquadratische rest is.

$$\left(\left(\frac{2}{M}\right)\right) = \left(\left(\frac{-2}{M}\right)\right) = 1,$$

erwijl uit  $2 = (1-i)(1+i)$  nog volgt

$$\left(\left(\frac{2}{M}\right)\right) = \left(\left(\frac{-2}{M}\right)\right) = 1.$$

Voor  $M = a + bi$  daarentegen, is

$$-m - j = -n + \frac{1}{4}b,$$

$$l + m = n + \frac{1}{4}b$$

en

$$n = \frac{a^2 + b^2 - 1}{8}.$$

Nu is blijkbaar  $\frac{a-1}{4} \cdot \frac{a+3}{4}$  even, dus  $\frac{(a-1)(a+3)}{8}$  door 4 deelbaar, waaruit volgt

$$\frac{a^2 - 1}{8} \equiv \frac{-a + 1}{4} \pmod{4},$$

en  $b$  door 4 deelbaar zijnde, is dus één der getallen door  $b$ ,  $b \pm 1$  door 8 deelbaar, derhalve  $\frac{b(b-4)}{8}$  door 4 deelbaar en

$$\frac{b^2}{8} \equiv \frac{b^2}{8} - \frac{b(b-4)}{8} = \pm \frac{1}{2}b,$$

zoodat

$$n \equiv \frac{1}{4}(-a + 1 \pm 2b) \pmod{4}$$

en ten slotte

$$\left(\left(\frac{1+i}{M}\right)\right) = \left(\left(\frac{-1-i}{M}\right)\right) = i^{\frac{a-1-b}{4}},$$

$$\left(\left(\frac{1-i}{M}\right)\right) = \left(\left(\frac{-1+i}{M}\right)\right) = i^{\frac{-a+1-b}{4}},$$

$$\left(\left(\frac{2}{M}\right)\right) = i^{-\frac{b}{2}}.$$

Is eindelijk  $\mu = 8n + 5$ ,  $M = a + bi$ , dan vindt men

$$\text{Karakter } (1+i) \equiv (1.1) + 2(1.2) + 3(1.3) = m + 2l + 3j \pmod{4}$$

$$\text{Karakter } (1-i) \equiv (3.1) + 2(3.2) + 3(3.3) = l + 2j + 3m \pmod{4}$$

Hierin is, alle congruenties betrekking hebbende op den modulus

$$m + 2l + 3j = 3n + \frac{1}{4}(-b + 6),$$

$$l + 2j + 3m = 3n + \frac{1}{4}(-b + 6) \equiv -n + \frac{1}{4}(-b + 6),$$

$$n = \frac{a^2 + b^2 - 5}{8};$$

$\frac{a-3}{4} \cdot \frac{a+1}{4}$  even zijnde, is  $\frac{(a-3)(a+1)}{8}$  door 4 deelbaar, evenzo

ook  $\frac{(b-2)(b+2)}{8}$ , dus heeft men

$$n \equiv \frac{a^2 + b^2 - 5}{8} - \frac{(a-3)(a+1)}{8} - \frac{b^2 - 4}{8} = \frac{1}{4}(a+1),$$

zoodat er ten slotte komt

$$m + 2l + 3j \equiv \frac{1}{4}(a - b + 11) \equiv (a - b - 5),$$

$$l + 2j + 3m \equiv \frac{1}{4}(-a - b + 5).$$

en hiermede

$$\left(\left(\frac{1+i}{a+bi}\right)\right) = i^{\frac{a-b-5}{4}}, \quad \left(\left(\frac{1-i}{a+bi}\right)\right) = i^{\frac{-a-b+5}{4}}.$$

Het karakter van  $-1$  gelijk twee zijnde, vindt men verder

$$\left(\left(\frac{-1-i}{a+bi}\right)\right) = i^{\frac{a-b+3}{4}}, \quad \left(\left(\frac{-1+i}{a+bi}\right)\right) = i^{\frac{-a-b-3}{4}}$$

en

$$\left(\left(\frac{2}{a+bi}\right)\right) = i^{-\frac{b}{2}}.$$

Hiermede is het quadratisch karakter van  $1+i$ , als ook dat van  $1-i$ ,  $-1-i$ ,  $-1+i$  ten opzichte van een primair priemgetal  $n$  in elk geval bepaald. De uitkomsten stemmen geheel overeen met die door Gauss in art. 63 en 64 van de *Theoria residuorum biquadratorum commentatio secunda* gegeven, en daar in art. 68—76 op geheel verschillende wijze bewezen.

16. Met betrekking tot de analogie van een groot gedeelte der voorafgaande beschouwingen met die van Gauss in art. 8 e. v. van zijn eerste verhandeling over de theorie der vierde-machtsresten valt het volgende op te merken.

Gauss beschouwt reële getallen, en de priemmodulus  $p$  is van de vorm  $4n+1$  terwijl de beide gevallen  $n=8n+1$ ,  $n=8n+5$  onder

norm  $\mu$  in de gevallen II en III van art. 4.

De getallen  $1, 2, 3, \dots, p-1$  worden nu bij Gauss in 4 klassen A, B, C, D verdeeld. De getallen dezer klassen door  $\alpha, \beta, \gamma, \delta$  aanduidende, is deze klassificatie gegrond op de congruenties

$$\begin{aligned} \alpha^{\frac{\mu-1}{4}} &\equiv 1 \\ \beta^{\frac{\mu-1}{4}} &\equiv f \\ \gamma^{\frac{\mu-1}{4}} &\equiv -1 \\ \delta^{\frac{\mu-1}{4}} &\equiv -f \end{aligned} \quad (\text{mod } \mu = p),$$

waarin  $f^2 \equiv -1 \pmod{p}$ , en voor  $\mu = a^2 + b^2$

$$a \equiv 1 \pmod{4}, \quad a + bf \equiv 0 \pmod{p}.$$

Voor  $p = \mu = 8n + 1$  hebben  $a$  en  $b$  dezelfde beteekenis als in het bovenstaande, voor  $p = 8n + 5$  verschillen  $a$  en  $b$  bij Gauss alleen in teeken met de waarden, die zij in het voorgaande hebben, waarvoor  $M = a + bi$  een primair complex priemgetal is

Laat men nu echter ook complexe getallen toe, dan is het duidelijk, dat de bovenstaande congruenties, die betrekking hebben op den modulus  $p = \mu$ , blijven gelden voor den modulus  $a + bi$ , zooda ook  $a + bf \equiv 0 \pmod{a + bi}$  is, waaruit blijkt  $f \equiv i \pmod{a + bi}$ , en dus

$$\alpha^{\frac{\mu-1}{4}} \equiv 1, \quad \beta^{\frac{\mu-1}{4}} \equiv i, \quad \gamma^{\frac{\mu-1}{4}} \equiv -1, \quad \delta^{\frac{\mu-1}{4}} \equiv -i \pmod{a + bi}.$$

De klassificatie van Gauss valt derhalve samen met die volgens het biquadratisch karakter 0, 1, 2, 3 met betrekking tot den modulus  $a + bi$ .

Inderdaad, de reële getallen  $1, 2, 3, \dots, p-1$  vormen voor den modulus  $a + bi$  een volledig systeem incongruente, niet door den modulus deelbare resten.

Vervangt men dan ook in de beide laatste voorbeelden van art. de complexe resten door de congruente reële getallen, wat met behulp van  $i \equiv 27 \pmod{-3-8i}$  en  $i \equiv 11 \pmod{-5+6i}$  zonder moeite kan geschieden, dan verkrijgt men

- A 1, 2, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72.  
 B 5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68  
 C 3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70  
 D 11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62

$$(\text{mod } -5 + 6i), \quad \mu = 61,$$

- A 1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58.  
 B 2, 7, 18, 23, 24, 26, 30, 32, 33, 40, 44, 50, 51, 53, 55.  
 C 3, 4, 5, 14, 19, 27, 36, 39, 41, 45, 46, 48, 49, 52, 60.  
 D 6, 8, 10, 11, 17, 21, 28, 29, 31, 35, 37, 38, 43, 54, 59.

volmaakt overeenkomende met de voorbeelden door Gauss gegeven in art. 11 der eerste verhandeling.

Alleen voor het geval I van art. 4, bestaat in de reële theorie van Gauss niets analoogs, wat daarmede samenhangt, dat men in dit geval uit reële getallen geen volledig restsysteem kan vormen.

De opmerking, dat de verdeeling in klassen A, B, C, D van Gauss in zijne eerste verhandeling identiek is met die volgens het biquadratisch karakter ten opzichte van den modulus  $a + bi$ , levert ook terstond het middel op, om al die theorema's te bewijzen, die door Gauss in zijne tweede verhandeling, art. 28, opgesteld zijn, en welke door inductie ontdekt werden, maar die tot nog toe, voor zoover ik zie niet werden bewezen.

Deze theorema's hebben betrekking op het voorkomen van een reëel priemgetal  $m$  in de vier klassen A, B, C, D, of na het voorgaande op het biquadratisch karakter van  $m$  ten opzichte van  $a + bi$  als modulus.

17. Ik laat nu hier de door Gauss in art. 28 opgestelde opmerkingen volgen. De priemmodulus  $p = \mu$  zij van den vorm  $4n + 1$  volgens de opmerking van het vorige artikel is het nu te doen om de bepaling van de waarde van het symbool

$$\left( \left( \frac{m}{a + bi} \right) \right),$$

waarin  $m$  een reëel priemgetal is; de omstandigheid, dat voor  $\mu = 8n + 1$   $a$  en  $b$  bij Gauss in teeken verschillen van de waarden in art. 14 heeft

het zulk een teeken genomen worden, dat het steeds  $\equiv 1 \pmod{4}$  is, dus negatief wanneer het positief genomen, van den vorm  $4k + 3 =$  is, terwijl een positief priemgetal van den vorm  $4k + 1$  door  $P$  zal aangeduid worden. De opmerkingen van Gauss kunnen nu aldus uitgedrukt worden

I. Is  $a \equiv 0 \pmod{m}$  dan is  $\left(\left(\frac{m}{a+bi}\right)\right) = \pm 1$ , en wel  $+1$  wanneer  $m$  van den vorm  $8r \pm 1$ , daarentegen  $-1$  wanneer  $m$  van den vorm  $8r \pm 3$  is.

II. Is  $a$  niet door  $m$  deelbaar, dan hangt de waarde van het symbool af alléén van het volkomen bepaalde getal  $x$ , dat voldoet aan de congruentie

$$b \equiv ax \pmod{m}.$$

Voor  $m = P$  kan  $x$  hier de volgende waarden aannemen

$$0, 1, 2, 3, \dots, P-1,$$

met uitzondering van de beide waarden  $f$  en  $P-f$ , die voldoen aan  $xy \equiv -1 \pmod{P}$ . Deze kunnen blijkbaar niet voorkomen, want uit  $xy \equiv -1$  zou volgen

$$b^2 \equiv -a^2 \text{ of } a^2 + b^2 = p \equiv 0 \pmod{P},$$

d. w. z.  $p$  zou door  $P$  deelbaar zijn.

Voor  $m = -Q$  daarentegen kan  $x$  alle waarden

$$0, 1, 2, 3, \dots, Q-1$$

aannemen.

Deze waarden van  $x$  kunnen nu in 4 klassen  $\alpha, \beta, \gamma, \delta$  verdeeld worden, zoodanig dat voor

$$b \equiv a\alpha \pmod{m} \text{ de waarde van het symbool } = 1,$$

$$b \equiv a\beta \quad " \quad " \quad " \quad " \quad " \quad " \quad " \quad = i,$$

$$b \equiv a\gamma \quad " \quad " \quad " \quad " \quad " \quad " \quad " \quad = -1,$$

$$b \equiv a\delta \quad " \quad " \quad " \quad " \quad " \quad " \quad " \quad = -i$$

is, of wat op hetzelfde neerkomt, dat in deze gevallen  $m$  respectievelijk tot de klassen A, B, C, D behoort.

Omtrent het aantal der getallen  $\alpha, \beta, \gamma, \delta$  geldt nu deze regel, dat drie dezer aantallen gelijk zijn, terwijl dan het vierde aantal één kleine

A behoort, en dat der  $\gamma$ 's, wanneer voor  $a \equiv 0 \pmod{m}$  tot C behoort.

De verdere opmerkingen van Gauss in art. 28 kunnen voor het oogenblik daargelaten worden, daar hun bewijs geen bezwaar onderzocht vindt, zoodra eenmaal het bovenstaande aangetoond is, waartoe ik nu overga.

18. Zij dan vooreerst  $m = -Q$ , volgens de reciprociteitswet is dan

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{Q}\right)\right)$$

en voor  $a \equiv 0 \pmod{Q}$

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{bi}{Q}\right)\right) = \left(\left(\frac{b}{Q}\right)\right) \left(\left(\frac{i}{Q}\right)\right) = i^{\frac{Q^2-1}{4}},$$

want  $\left(\left(\frac{b}{Q}\right)\right) = 1$ ; immers men heeft

$$\left(\left(\frac{b}{Q}\right)\right) \equiv b^{\frac{Q^2-1}{4}} \pmod{Q}$$

en daar  $Q$  van den vorm  $4r+3$ , en dus  $\frac{Q^2-1}{4} = (Q-1) \frac{Q+1}{4}$  een veelvoud van  $Q-1$  is, zoo volgt uit het theorema van Fermat

$$\left(\left(\frac{b}{Q}\right)\right) = 1.$$

Voor  $Q = 8n+3$  volgt nu

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = -1,$$

voor  $Q = 8n+7$

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = +1.$$

Voor  $m = P = (A+Bi)(A-Bi)$  daarentegen, waarin  $A+Bi$  en  $A-Bi$  de primaire factoren van  $P$  zijn, volgt uit de reciprociteitswet

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{A+Bi}\right)\right) \left(\left(\frac{a+bi}{A-Bi}\right)\right)$$

en voor  $a \equiv 0 \pmod{P}$

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{bi}{A+Bi}\right)\right) \left(\left(\frac{bi}{A-Bi}\right)\right) = \left(\left(\frac{-bi}{A+Bi}\right)\right) \left(\left(\frac{+bi}{A-Bi}\right)\right) \left(\left(\frac{-1}{A+Bi}\right)\right).$$

$$\left(\left(\frac{\alpha + \beta i}{A + Bi}\right)\right) \left(\left(\frac{\alpha - \beta i}{A - Bi}\right)\right) = 1,$$

dus

$$\left(\left(\frac{P}{a + bi}\right)\right) = \left(\left(\frac{-1}{A + Bi}\right)\right) = (-1)^{\frac{P-1}{4}},$$

of voor  $P = 8n + 1$

$$\left(\left(\frac{P}{a + bi}\right)\right) = 1$$

en voor  $P = 8n + 5$

$$\left(\left(\frac{P}{a + bi}\right)\right) = -1.$$

Hiermede is dus het in het voorgaande art. onder I gezegde geheel bewezen.

19. Onderstellen wij dan nu, dat  $a$  niet door  $m$  deelbaar is, en beschouwen wij eerst het eenvoudigste geval

$$m = -Q,$$

dan is dus

$$\left(\left(\frac{-Q}{a + bi}\right)\right) = \left(\left(\frac{a + bi}{Q}\right)\right)$$

en voor  $b \equiv ax \pmod{Q}$

$$\left(\left(\frac{-Q}{a + bi}\right)\right) = \left(\left(\frac{a(1 + xi)}{Q}\right)\right) = \left(\left(\frac{1 + xi}{Q}\right)\right),$$

daar  $\left(\left(\frac{a}{Q}\right)\right) = 1$  is, zooals reeds in het voorgaand artikel bewezen werd. Uit de verkregen uitkomst

$$\left(\left(\frac{-Q}{a + bi}\right)\right) = \left(\left(\frac{1 + xi}{Q}\right)\right)$$

blijkt nu reeds, dat de waarde van het symbool links, alleen van het getal  $x$  afhangt, welk getal de  $Q$  waarden

$$0, 1, 2, 3, \dots, Q - 1$$

kan aannemen.

Wij hebben dus nu nog slechts deze vraag te beantwoorden



hoeveel der getallen

$$1, 1 + i, 1 + 2i, 1 + 3i, \dots, 1 + (Q - 1)i$$

behooren er dan respectievelijk tot de klassen A, B, C, D?

Ik merk hiertoe vooreerst op, dat als een volledig systeem niet door  $Q$  deelbare resten de getallen

$$\alpha + \beta i$$

genomen kunnen worden, waarin  $\alpha$  en  $\beta$  de waarden  $0, 1, 2, 3, \dots, Q - 1$  doorloopen, met uitzondering der combinatie  $\alpha = 0, \beta = 0$ ; en ten tweede, dat de getallen

$$1, 2, 3, \dots, q - 1$$

alle tot A behooren, zoodat wanneer

$$\alpha' + \beta' i$$

tot eene zekere klasse behoort, ook

$$2(\alpha' + \beta' i), 3(\alpha' + \beta' i), \dots, (q - 1)(\alpha' + \beta' i)$$

tot diezelfde klasse behooren, alle welke getallen door het weglaten van veelvouden van  $q$  weder tot den vorm  $\alpha + \beta i$ , waarin  $\alpha$  en  $\beta$  kleiner dan  $q$  zijn, teruggebracht kunnen worden. Nu zijn de resten van

$$\alpha', 2\alpha', 3\alpha', \dots, (q - 1)\alpha',$$

zoolang  $\alpha'$  niet gelijk nul is, volgens den modulus  $q$  in zekere volgorde met de getallen

$$1, 2, 3, \dots, q - 1$$

congruent.

In de groep der  $q - 1$  getallen

$$\alpha' + \beta' i, 2(\alpha' + \beta' i), \dots, (q - 1)(\alpha' + \beta' i),$$

die alle tot dezelfde klasse behooren, komt er dus één voor, congruent met een der getallen

$$1 + xi \quad (x = 0, 1, 2, \dots, q - 1).$$

Nu is het aantal getallen van elke klasse

$$\frac{q^2 - 1}{4} = (q - 1) \times \frac{q + 1}{4},$$

een veelvoud van  $q - 1$ , en de  $q - 1$  getallen zonder reëel gedeelte

$$i, 2i, 3i, \dots, (q - 1)i$$

behooren voor  $q = 8n + 7$  tot A, voor  $q = 8n + 3$  tot C.

Daar men nu alle getallen van elke klasse, waarvan het reëel gedeelte niet gelijk nul is, op bovenstaande wijze in groepen van  $q - 1$  getallen kan vereenigen, zoodanig dat er in elke groep één getal met het reëele gedeelte 1 voorkomt, zoo volgt, dat voor  $Q = 8n + 3$  er in de klassen A, B, C, D respectievelijk

$$\frac{q-3}{4}, \quad \frac{q+1}{4}, \quad \frac{q+1}{4}, \quad \frac{q+1}{4}$$

getallen  $1 + xi$  voorkomen.

Voor  $Q = 8n + 3$  zijn deze aantallen

$$\frac{q+1}{4}, \quad \frac{q+1}{4}, \quad \frac{q-3}{4}, \quad \frac{q+1}{4},$$

terwijl volgens art. 18 in het geval  $a \equiv 0 \pmod{Q}$  voor  $Q = 8n + 3$  of  $Q = 8n + 3$ ,  $Q$  respectievelijk tot de klassen A en C behoorde.

Alles wat op het geval  $m = -Q$  betrekking had, is dus hiermede afgehandeld.

20. Voor  $m = P = (A + Bi)(A - Bi)$  vonden wij reeds

$$\left( \left( \frac{P}{a + bi} \right) \right) = \left( \left( \frac{a + bi}{A + Bi} \right) \right) \left( \left( \frac{a + bi}{A - Bi} \right) \right)$$

en dus wanneer

$$b \equiv ax \pmod{P},$$

neeft men

$$\left( \left( \frac{P}{a + bi} \right) \right) = \left( \left( \frac{1 + xi}{A + Bi} \right) \right) \left( \left( \frac{1 + xi}{A - Bi} \right) \right) \left( \left( \frac{a}{A + Bi} \right) \right) \left( \left( \frac{a}{A - Bi} \right) \right)$$

of daar, volgens een reeds in art. 18 gemaakte opmerking, het product der beide laatste factoren rechts gelijk 1 is,

$$\left( \left( \frac{P}{a + bi} \right) \right) = \left( \left( \frac{1 + xi}{A + Bi} \right) \right) \left( \left( \frac{1 + xi}{A - Bi} \right) \right),$$

waaruit reeds blijkt, dat de waarde van het symbool links alleen van het getal  $x$  afhangt, zoodat nog slechts de volgende vraag te beantwoorden blijft: voor hoeveel waarden van  $1 + xi$  neemt

$$\left( \left( \frac{1 + xi}{A + Bi} \right) \right) \left( \left( \frac{1 + xi}{A - Bi} \right) \right)$$

incongruente niet door den modulus  $A + Bi$  deelbare resten, en breng deze volgens hun biquadratisch karakter tot 4 groepen A, B, C, D. Hierbij denk ik mij elke rest zoo gekozen, dat het reële deel gelijk 1, en de factor van  $i$  kleiner dan  $P$  is.

Men kan dit aldus voorstellen :

$$(\text{mod } A + Bi), \quad A^2 + B^2 = P.$$

Klasse A	$\alpha = 1 + a i$
B	$\beta = 1 + b i$
C	$\gamma = 1 + c i$
D	$\delta = 1 + d i$

De getallen  $a, b, c, d$  in hun geheel stemmen overeen met

$$0, 1, 2, 3, \dots, (P-1),$$

behalve dat de waarde  $f$ , die congruent  $i$  is ontbreekt, want  $1 + fi \equiv (\text{mod } A + Bi)$ .

Evenzoo met  $A - Bi$  handelende, ziet men gemakkelijk, dat de klassificatie deze zal zijn :

$$(\text{mod } A - Bi), \quad A^2 + B^2 = P.$$

Klasse A	$1 + (P - a) i$
B	$1 + (P - d) i$
C	$1 + (P - c) i$
D	$1 + (P - b) i$

want gelijktijdig heeft men

$$(1 + xi)^{\frac{P-1}{4}} - i^p = (A + Bi)(C + Di),$$

$$(1 - xi)^{\frac{P-1}{4}} - i^{3p} = (A - Bi)(C - Di).$$

Heeft dus  $1 + xi$  volgens den modulus  $A + Bi$  het karakter  $\rho$  dan heeft  $1 - xi \equiv 1 + (P - x)i$  volgens den modulus  $A - Bi$  het karakter  $3\rho$ .

21. Zal nu

$$\left( \frac{1 + xi}{A + Bi} \right) \left( \frac{1 + xi}{A - Bi} \right)$$

$$\left(\left(\frac{1 + xi}{A + Bi}\right)\right)$$

een der waarden  $1, i, -1, -i$  heeft, tegelijkertijd

$$\left(\left(\frac{1 + xi}{A - Bi}\right)\right)$$

een der waarden  $1, -i, -1, i$  aannemen, of op de beide verdelingen in klassen lettende: wanneer  $x$  respectievelijk tot  $a, b, c$ , behoort, dan moet tegelijkertijd ook  $p - x$  tot de getallen  $a, b, c$ , behooren. Men kan dus zeggen, dat het aantal der waarden van waarvoor

$$\left(\left(\frac{1 + xi}{A + Bi}\right)\right) \left(\left(\frac{1 + xi}{A - Bi}\right)\right) = 1$$

wordt, gelijk is aan de som van de aantallen oplossingen der congruenties

$$a + a' \equiv 0,$$

$$b + b' \equiv 0,$$

$$c + c' \equiv 0,$$

$$d + d' \equiv 0,$$

ten opzichte van den modulus  $P$ , of wat op hetzelfde neerkomt, ten opzichte van den modulus  $A + Bi$ .

Men bedenke hierbij, dat wel de voor  $x$  uitgesloten waarde  $p - x$  onder  $a, b, c, d$  voorkomt, maar dat deze waarde toch in geen der bovenstaande congruenties kan optreden, omdat dit zoude vereischen dat ook  $f$  voorkwam onder de getallen  $a, b, c, d$ , wat niet het geval is.

Nu is  $a = 1 + ai$ , zoodat de voorgaande congruenties na vermenigvuldiging met  $i$ , overgaan in

$$a + a' \equiv 2$$

$$\beta + \beta' \equiv 2$$

$$\gamma + \gamma' \equiv 2$$

$$\delta + \delta' \equiv 2.$$

$$(\text{mod } A + Bi).$$

Behoort  $\frac{p-1}{2}$  tot de klasse  $A$ , dan gaan de voorgaande congruenties door vermenigvuldiging met  $\frac{p-1}{2}$  over in

$$\begin{aligned}\beta + \beta' + 1 &\equiv 0 \\ \gamma + \gamma' + 1 &\equiv 0 \\ \delta + \delta' + 1 &\equiv 0\end{aligned} \pmod{A + Bi},$$

zoodat de som van het aantal oplossingen dezer congruenties gelijk is aan het aantal waarden van  $x$ , die

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right) \left(\left(\frac{1+xi}{A-Bi}\right)\right)$$

gelijk 1 maken.

Maar zooals men zich onmiddellijk overtuigt, blijft dit resultaat hetzelfde, ook wanneer  $\frac{p-1}{2}$  tot de klassen B, C, D behoort. Behoort bijv.  $\frac{p-1}{2}$  tot B, dan volgt uit  $\alpha + \alpha' \equiv 2$  door vermenigvuldiging met  $\frac{p-1}{2}$

$$\beta + \beta' + 1 \equiv 0,$$

en uit  $\beta + \beta' \equiv \gamma + \gamma' \equiv \delta + \delta' \equiv 2$  respectievelijk

$$\gamma + \gamma' + 1 \equiv 0, \quad \delta + \delta' + 1 \equiv 0, \quad \alpha + \alpha' + 1 \equiv 0.$$

Noemt men de aantallen der waarden van  $x$ , die respectievelijk  $\left(\left(\frac{1+xi}{A+Bi}\right)\right) \left(\left(\frac{1+xi}{A-Bi}\right)\right)$  gelijk 1,  $i$ ,  $-1$ ,  $-i$  maken,  $t, u, v, w$ , dan is dus  $t$  de som van de aantallen oplossingen der congruenties

$$\begin{aligned}\alpha + \alpha' + 1 &\equiv 0 \\ \beta + \beta' + 1 &\equiv 0 \\ \gamma + \gamma' + 1 &\equiv 0 \\ \delta + \delta' + 1 &\equiv 0\end{aligned} \pmod{A + Bi}.$$

Geheel op dezelfde wijze vindt men, dat  $u$  de som is van de aantallen oplossingen der congruenties

$$\begin{aligned}\alpha + \delta + 1 &\equiv 0, \\ \beta + \alpha + 1 &\equiv 0, \\ \gamma + \beta + 1 &\equiv 0, \\ \delta + \gamma + 1 &\equiv 0,\end{aligned}$$

$$\begin{array}{ll}
\alpha + \gamma + 1 \equiv 0, & \alpha + \beta + 1 \equiv 0, \\
\beta + \delta + 1 \equiv 0, & \text{en } \beta + \gamma + 1 \equiv 0, \\
\gamma + \alpha + 1 \equiv 0, & \gamma + \delta + 1 \equiv 0, \\
\delta + \beta + 1 \equiv 0, & \delta + \alpha + 1 \equiv 0,
\end{array}$$

te beschouwen heeft.

Is dus  $P = 8n + 1$ , dan heeft men volgens art. 7 en 8

$$t = (0.0) + (1.1) + (2.2) + (3.3) = h + l + k + j = 2n - 1,$$

$$u = (0.3) + (1.0) + (2.1) + (3.2) = l + j + m + m = 2n,$$

$$v = (0.2) + (1.3) + (2.0) + (3.1) = k + m + k + m = 2n,$$

$$w = (0.1) + (1.2) + (2.3) + (3.0) = j + m + m + l = 2n,$$

en voor  $P = 8n + 5$  volgens art. 13

$$t = (0.2) + (1.3) + (2.0) + (3.1) = k + j + h + l = 2n + 1,$$

$$u = (0.1) + (1.2) + (2.3) + (3.0) = j + l + m + m = 2n + 1,$$

$$v = (0.0) + (1.1) + (2.2) + (3.3) = h + m + h + m = 2n,$$

$$w = (0.3) + (1.0) + (2.1) + (3.2) = l + m + m + j = 2n + 1.$$

22. Al het voorgaande samenstellende, hebben dus de kenmerken om te onderscheiden of een reëel priemgetal tot de klassen A, B, behoort, wanneer de modulus  $p$  van den vorm  $4n + 1$  en  $a + b i$  primaire complexe priemfactor van  $p$  is, de volgende gedaante:

Het priemgetal  $P = 8n + 1$  behoort tot

A voor $a \equiv 0, \quad b \equiv a\alpha$	Aantal der $a$ 's $= 2n - 1,$
B voor $b \equiv a\beta$	(mod P). " " $\beta$ 's $= 2n,$
C voor $b \equiv a\gamma$	" " $\gamma$ 's $= 2n,$
D voor $b \equiv a\delta$	" " $\delta$ 's $= 2n.$

Het priemgetal  $P = 8n + 5$  behoort tot

A voor $b \equiv a\alpha$	Aantal der $a$ 's $= 2n + 1,$
B voor $b \equiv a\beta$	(mod P). " " $\beta$ 's $= 2n + 1,$
C voor $b \equiv a\gamma, \quad a \equiv 0$	" " $\gamma$ 's $= 2n,$
D voor $b \equiv a\delta$	" " $\delta$ 's $= 2n + 1.$

Het priemgetal  $-Q = -(8n + 3)$  behoort tot

A voor $b \equiv a\alpha$	Aantal der $a$ 's $= 2n + 1,$
B voor $b \equiv a\beta$	(mod Q). " " $\beta$ 's $= 2n + 1,$
C voor $b \equiv a\gamma, \quad a \equiv 0$	" " $\gamma$ 's $= 2n,$
D voor $b \equiv a\delta$	" " $\delta$ 's $= 2n + 1.$

het priemgetal  $-Q = -(8n+7)$  behoort tot

A voor  $b \equiv a \alpha, \alpha \equiv 0$

Aantal der  $\alpha$ 's  $= 2n+1$ ,

B voor  $b \equiv a \beta \pmod{Q}$ . „ „  $\beta$ 's  $= 2n+2$ ,

C voor  $b \equiv a \gamma$  „ „  $\gamma$ 's  $= 2n+2$ ,

D voor  $b \equiv a \delta$  „ „  $\delta$ 's  $= 2n+2$ .

Ik voeg hierbij nog de volgende opmerkingen van Gauss (art. 28) waarvan het bewijs na al het voorgaande niet het minste bezwaar oplevert.

1. Het getal 0 behoort altijd tot de  $\alpha$ 's, en de getallen  $-\alpha, -\beta, -\gamma, -\delta$  behooren  $\pmod{m}$  respectievelijk tot de  $\alpha$ 's,  $\delta$ 's,  $\gamma$ 's en  $\beta$ 's.

2. Voor  $P = 8n+1, Q = 8n+7$  behooren de waarden van  $\frac{1}{\alpha}, \frac{1}{\beta}, \frac{1}{\gamma}, \frac{1}{\delta} \pmod{m}$  respectievelijk tot de  $\alpha$ 's,  $\delta$ 's,  $\gamma$ 's,  $\beta$ 's; en voor  $P = 8n+5, Q = 8n+3$  behooren deze waarden respectievelijk tot de  $\gamma$ 's,  $\beta$ 's,  $\alpha$ 's,  $\delta$ 's.

### DERDE-MACHTSRESTEN.

23. Nu tot de derde-machtsresten overgaande, is het noodig een en ander omtrent de theorie der geheele getallen van den vorm  $a+b\varrho$  in herinnering te brengen;  $\varrho$  is hierin een complexe derde-machtswortel der eenheid, dus  $1+\varrho+\varrho^2=0$ .

Zooals dan bekend is, gelden ook in deze theorie omtrent de deelbaarheid der getallen, hunne ontbinding in priemfactoren, het bestaan van primitieve wortels der priemgetallen enz. geheel analoge theorema's als die in de gewone theorie der reële getallen, en verreweg het grootste gedeelte der onderzoekingen in de vier eerste sectiën der Disquisitiones arithmeticae kunnen bijna onveranderd ook voor de theorie der geheele getallen  $a+b\varrho$  doorgevoerd worden.

Het product van twee geconjugeerde getallen  $a+b\varrho$  en  $a+b\varrho^2$

$$(a+b\varrho)(a+b\varrho^2) = a^2 - ab + b^2$$

heet de norm van het getal  $a+b\varrho$  en zal steeds door  $\mu$  aangeduid worden.

Het getal 3 is in deze theorie geen priemgetal, want

$$3 = (1-\varrho)(1-\varrho^2) = -\varrho^2(1-\varrho)^2$$

ten eerste de reële priemgetallen van den vorm  $3n - 1$ , de norm is dan gelijk  $(3n - 1)^2$ ;

ten tweede de complexe priemfactoren van de reële priemgetallen van den vorm  $3n + 1$ . Dit reële priemgetal is dan te gelijk de norm van den complexen priemfactor.

Bijv. is

$$7 = (2 + 3\varrho)(2 + 3\varrho^2) = (2 + 3\varrho)(-1 - 3\varrho).$$

De priemgetallen  $2 + 3\varrho$ ,  $-1 - 3\varrho$  hebben beide 7 tot norm.

In beide gevallen is dus de norm van den vorm  $3k + 1$ .

Verder is het voldoende alleen primaire priemgetallen te beschouwen, waarbij ik mij van dit woord in den zin van Eisenstein (Crelle's Journal, 27, p. 301) zal bedienen, zoodat  $a + b\varrho$  primair heet, wanneer  $a + 1$  en  $b$  beide door 3 deelbaar zijn. De reële priemgetallen van den vorm  $3n - 1$  moeten dus positief genomen worden om primair te zijn.

Zij dan  $M$  een primair priemgetal,  $\mu$  de norm van den vorm  $3n + 1$ . Een volledig stelsel incongruente, niet door den modulus  $M$  deelbare resten bevat dan  $\mu - 1 = 3n$  getallen. Deze getallen kunnen tot 3 klassen, elk  $\mu$  getallen bevattende, gebracht worden al naar dat hunne  $\left(\frac{\mu - 1}{3}\right)^{\text{de}}$  macht (mod  $M$ ) congruent is met 1,  $\varrho$  of  $\varrho^2$ . Deze verdeling kan aldus voorgesteld worden:

A	$\alpha, \alpha', \alpha'', \dots$
B	$\beta, \beta', \beta'', \dots$
C	$\gamma, \gamma', \gamma'', \dots$

waarin dus

$$\alpha^{\frac{\mu-1}{3}} \equiv 1, \quad \beta^{\frac{\mu-1}{3}} \equiv \varrho, \quad \gamma^{\frac{\mu-1}{3}} \equiv \varrho^2 \pmod{M}.$$

Het cubisch karakter der getallen  $\alpha, \alpha', \alpha'', \dots$  is 0, dat der getallen  $\beta, \beta', \dots$  is 1, dat der getallen  $\gamma, \gamma', \dots$  is 2.

Het zal intusschen ook gemakkelijk zijn, van het symbool van Eisenstein gebruik te maken, en dus te schrijven

$$\left[\frac{\alpha}{M}\right] = 1, \quad \left[\frac{\beta}{M}\right] = \varrho, \quad \left[\frac{\gamma}{M}\right] = \varrho^2.$$



het doel van de eerstvolgende beschouwingen is nu de bepaling van het cubisch karakter van  $1 - \varrho$ , of wel de bepaling van de waarde van het symbool  $\left[ \frac{1 - \varrho}{M} \right]$ .

24. Door bij alle getallen van A, B, C de eenheid op te tellen ontstaan de 3 groepen van getallen A', B', C'

$$\begin{array}{lll} A' & a + 1, & a' + 1, & a'' + 1, \dots \\ B' & \beta + 1, & \beta' + 1, & \beta'' + 1, \dots \\ C' & \gamma + 1, & \gamma' + 1, & \gamma'' + 1, \dots \end{array}$$

en ik noem nu (0.0), (0.1), (0.2) de aantallen getallen van A', die respectievelijk congruent zijn met getallen van A, B, C; (1.0), (1.1), (1.2) de aantallen getallen van B', die respectievelijk congruent zijn met getallen van A, B, C; eindelijk (2.0), (2.1), (2.2) de aantallen getallen van C', die respectievelijk congruent zijn met getallen van A, B, C.

Al deze getallen kunnen in het schema S vereenigd worden

$$\begin{array}{lll} (0.0) & (0.1) & (0.2) \\ (1.0) & (1.1) & (1.2) \\ (2.0) & (2.1) & (2.2) \end{array}$$

en met de bepaling van deze getallen is ook onmiddellijk het cubisch karakter van  $1 - \varrho$  gevonden. Want uit de blijkbaar identieke congruenties

$$\begin{aligned} (x - a)(x - a')(x - a'') \dots &\equiv x^{\frac{\mu - 1}{3}} - 1 \\ (x - \beta)(x - \beta')(x - \beta'') \dots &\equiv x^{\frac{\mu - 1}{3}} - \varrho \pmod{M} \\ (x - \gamma)(x - \gamma')(x - \gamma'') \dots &\equiv x^{\frac{\mu - 1}{3}} - \varrho^2 \end{aligned}$$

volgt voor  $x = -1$ , daar  $\frac{\mu - 1}{3}$  even is (behalve voor  $M = 2$ , welk geval uit te zonderen is),

$$\begin{aligned} (\beta + 1)(\beta' + 1)(\beta'' + 1) \dots &\equiv 1 - \varrho \pmod{M}, \\ (\gamma + 1)(\gamma' + 1)(\gamma'' + 1) \dots &\equiv 1 - \varrho^2 \pmod{M}, \end{aligned}$$

waaruit onmiddellijk volgt

$$\begin{aligned} \left[ \frac{1 - \varrho}{M} \right] &= \varrho^{(1.1) + 2(1.2)}, \\ \left[ \frac{1 - \varrho^2}{M} \right] &= \varrho^{(2.1) + 2(2.2)}. \end{aligned}$$

25. Het getal  $-1$  behoort, als volkomen derde-macht tot de klasse A, en de getallen  $\alpha$  en  $-\alpha$ ,  $\beta$  en  $-\beta$ ,  $\gamma$  en  $-\gamma$  komen tegelijkertijd in de klassen A, B, C voor.

Met behulp van deze opmerking overtuigt men zich nu dadelijk, dat

het teeken	voorstelt het aantal oplossingen van
(0.0)	$\alpha + \alpha' + 1 \equiv 0$
(0.1)	$\alpha + \beta + 1 \equiv 0$
(0.2)	$\alpha + \gamma + 1 \equiv 0$
(1.0)	$\beta + \alpha + 1 \equiv 0$
(1.1)	$\beta + \beta' + 1 \equiv 0 \pmod{M},$
(1.2)	$\beta + \gamma + 1 \equiv 0$
(2.0)	$\gamma + \alpha + 1 \equiv 0$
(2.1)	$\gamma + \beta + 1 \equiv 0$
(2.2)	$\gamma + \gamma' + 1 \equiv 0$

zoodat men heeft

$$(0.1) = (1.0), \quad (0.2) = (2.0), \quad (1.2) = (2.1).$$

Is  $xy \equiv 1 \pmod{M}$  en behoort  $x$  tot A, dan behoort blijkbaar ook  $y$  tot A, behoort echter  $x$  tot B of C, dan behoort  $y$  respectievelijk tot C of B, wat men kan uitdrukken door te schrijven

$$\alpha \alpha' \equiv 1, \quad \beta \gamma \equiv 1 \pmod{M}.$$

Uit

$$\begin{aligned} \gamma(\alpha + \beta + 1) &\equiv \gamma' + 1 + \gamma, \\ \beta(\alpha + \gamma + 1) &\equiv \beta' + 1 + \beta, \end{aligned}$$

besluit men nu tot deze betrekkingen

$$(0.1) = (2.2), \quad (0.2) = (1.1),$$

zoodat het schema S dezen vorm heeft

$$\begin{array}{ccc} h & j & k \\ j & k & l \\ k & l & j. \end{array}$$

Daar  $-1$  tot A, dus 0 tot A' behoort, maar behalve dit getal van A' overigens alle getallen van A', B', C' elk met één getal van A, B of C congruent zijn, zoo volgt verder

$$h + j + k = n - 1,$$

De beschouwing van het aantal oplossingen der congruentie

$$\alpha + \beta + \gamma + 1 \equiv 0 \pmod{M},$$

waarin  $\alpha, \beta, \gamma$  respectievelijk uit de klassen A, B, C te kiezen zijn levert eindelijk nog eene betrekking tusschen  $h, j, k, l$ . Neemt men namelijk eerst voor  $\alpha$  de getallen van A, dan verkrijgt men voor dit aantal

$$hl + jj + kk.$$

Neemt men daarentegen achtereenvolgens voor  $\beta$  alle getallen van B, dan vindt men voor ditzelfde aantal

$$jk + kl + lj$$

dus is

$$0 = hl + jj + kk - jk - kl - lj.$$

26. Elimineert men uit deze laatste vergelijking  $h$  met behulp van  $h = l - 1$ , dan is

$$0 = l(l - 1) + jj + kk - jk - kl - lj,$$

welke vergelijking met 4 vermenigvuldigd, wegens

$$(j + k)^2 + 3(j - k)^2 = 4(jj + kk - jk)$$

den vorm aanneemt

$$0 = 4l^2 - 4l + (j + k)^2 + 3(j - k)^2 - 4l(k + j).$$

Daar  $l = n - (j + k)$  is, heeft men door met 9 te vermenigvuldigen

$$36n = 36l^2 + 9(j + k)^2 + 27(j - k)^2 - 36l(j + k) + 36(j + k);$$

tegelijk is

$$24n = 24(j + k + l),$$

dus vindt men door aftrekking

$$12n = 36l^2 + 9(j + k)^2 + 27(j - k)^2 - 36l(j + k) + 12(j + k) - 24l,$$

of wel

$$12n + 4 = 4\mu = (6l - 3j - 3k - 2)^2 + 27(j - k)^2.$$

Stellen wij nu

aldus uitdrukken

$$\begin{aligned}9h &= 3n + A - 7, \\18j &= 6n - A + 3B - 2, \\18k &= 6n - A - 3B - 2, \\9l &= 3n + A + 2.\end{aligned}$$

Om nog  $A$  en  $B$  te bepalen zijn nu twee gevallen te onderscheiden

27. Is vooreerst  $M$  reëel van den vorm  $3n - 1$ , dus  $\mu = M^2$ , dan volgt uit

$$4\mu = 4M^2 = A^2 + 3B^2,$$

dat  $A = \pm 2M$ ,  $B = 0$  is. Want was  $B$  niet gelijk nul, dan zou men een geheel getal  $x$  kunnen bepalen, zóó dat

$$A \equiv Bx \pmod{M},$$

waaruit volgt

$$A^2 \equiv -3B^2 \equiv B^2x^2 \pmod{M}$$

dus

$$x^2 \equiv -3 \pmod{M},$$

wat onmogelijk is, daar men weet, dat  $-3$  niet-rest is van  $M$ .

Stellig is dus  $B = 0$ ,  $A = \pm 2M$ . Maar ook het teeken van  $A$  volgt onmiddellijk uit de opmerking, dat  $A \equiv 1 \pmod{3}$ , en  $M$  als priemgetal  $\equiv -1 \pmod{3}$  is; waaruit dus blijkt

$$A = 2M$$

en ten slotte

$$\begin{aligned}9h &= 3n + 2M - 7, \\9j &= 9k = 3n - M - 1, \\9l &= 3n + 2M + 2.\end{aligned}$$

28. Is in de tweede plaats  $M = a + b\varrho$  een primaire complex priemfactor van een reëel priemgetal  $p$  van den vorm  $3n + 1$ , dan is

$$4\mu = (2a - b)^2 + 3b^2 = A^2 + 3B^2$$

en daar  $a + b\varrho$  primair is,  $a + 1 \equiv b \equiv 0 \pmod{3}$ .

Nu is ook  $B$  door 3 deelbaar en daar, zooals gemakkelijk te bewijzen valt,  $4\mu$  slechts op één wijze voorgesteld kan worden als de som van een kwadraat en het 27-voud van een tweede kwadraat, zoo volgt

$$A = 2a - b, \quad B = \pm b.$$

Het teeken van A wordt namelijk weder bepaald door  $A \equiv 1 \pmod{3}$

Om nog het teeken van B te bepalen, dient de volgende beschouwing; doorloopt  $z$  alle getallen van A, B en C, dan vindt men op geheel dezelfde wijze als in art. 12,

$$\Sigma(z^3 + 1)^{\frac{\mu-1}{3}} \equiv -2 \equiv 3(h + j\varrho + k\varrho^2) \pmod{M},$$

of

$$-2 \equiv 3[(h - k) + \varrho(j - k)]$$

en nu  $h, j, k$  door A en B uitdrukken, en voor A de waarde  $2a - b$  schrijvende, verkrijgt men na eene kleine herleiding

$$0 \equiv 2a - b + B + 2B\varrho \pmod{M = a + b\varrho},$$

waaruit blijkt, dat  $B = b$  is

Nadat op deze wijze A en B gevonden zijn, heeft men

$$9h = 3n + 2a - b - 7,$$

$$9j = 3n - a + 2b - 1,$$

$$9k = 3n - a - b - 1,$$

$$9l = 3n + 2a - b + 2.$$

29. Volgens art. 24 is nu het cubisch karakter van  $1 - \varrho$  volgens den modulus 3 congruent met

$$(1.1) + 2(1.2) \equiv k - l,$$

dat van  $1 - \varrho^2$  congruent met

$$(2.1) + 2(2.2) \equiv l - j,$$

plus wanneer M reëel van den vorm  $3n - 1$  is, heeft men volgens art. 27

$$\text{Karakter}(1 - \varrho) \equiv -\frac{M+1}{3},$$

$$\text{Karakter}(1 - \varrho^2) \equiv +\frac{M+1}{3},$$

of wel

$$\left[\frac{1-\varrho}{M}\right] = \varrho^{-\frac{M+1}{3}}, \quad \left[\frac{1-\varrho^2}{M}\right] = \varrho^{+\frac{M+1}{3}},$$

waaruit nog volgt

is daarentegen  $M = a + b\varrho$  een primaire complexe factor van een reëel priemgetal van den vorm  $3n + 1$ , dan is volgens de waarde in art. 28 gevonden

$$\text{Karakter } (1 - \varrho) \equiv -\frac{a+1}{3},$$

$$\text{Karakter } (1 - \varrho^2) \equiv \frac{a-b+1}{3},$$

of

$$\left[ \frac{1 - \varrho}{a + b\varrho} \right] = \varrho^{-\frac{a+1}{3}}, \quad \left[ \frac{1 - \varrho^2}{a + b\varrho} \right] = \varrho^{\frac{a-b+1}{3}}, \quad \left[ \frac{3}{a + b\varrho} \right] = \varrho^{-\frac{b}{3}}.$$

Deze resultaten verschillen niet wezenlijk van die door Eisenstein gegeven in het 28<sup>ste</sup> deel van Crelle's Journal, p. 28 e. v.

30. Omtrent het geval, dat het priemgetal  $M$  een factor is van een reëel priemgetal  $p$  van den vorm  $3n + 1$ , moge nog het volgende opgemerkt worden.

Daar in  $M = a + b\varrho$ ,  $a$  en  $b$  geen gemeenen deeler hebben en derhalve ook  $b$  en  $a - b$  relatief priem zijn, zoo kan men altijd twee geheele getallen  $\alpha$  en  $\beta$  vinden, zoodanig dat

$$b\alpha + (a - b)\beta = 1$$

wordt, en dan is

$$(a + b\varrho)(\alpha + \beta\varrho) = a\alpha - b\beta + \varrho,$$

derhalve

$$\varrho \equiv b\beta - a\alpha \pmod{M = a + b\varrho}.$$

Hieruit volgt onmiddellijk, dat elk geheel getal  $c + d\varrho$  volgens de modulus  $a + b\varrho$  congruent is met een reëel getal, welk reëel getal kleiner dan de modulus  $\mu = p$  aangenomen kan worden, zoodat de reële getallen

$$0, 1, 2, 3, \dots, \mu - 1$$

een volledig restsysteem vormen. Verdeelt men nu deze reële getallen (met uitzondering van 0) volgens hun cubisch karakter in drie klassen

A	$\alpha, \alpha', \alpha'', \dots$
B	$\beta, \beta', \beta'', \dots$
C	$\gamma, \gamma', \gamma'', \dots$

$$\alpha^{\frac{\mu-1}{3}} - 1 \equiv \beta^{\frac{\mu-1}{3}} - f \equiv \gamma^{\frac{\mu-1}{3}} - f^2 \equiv 0 \pmod{M = a + b\varrho},$$

en daar

$$\alpha^{\frac{\mu-1}{3}} - 1, \beta^{\frac{\mu-1}{3}} - f, \gamma^{\frac{\mu-1}{3}} - f^2$$

reële getallen zijn, zoo moeten zij niet alleen door  $a + b\varrho$  maar ook door den modulus

$$p = \mu = (a + b\varrho)(a + b\varrho^2)$$

deelbaar zijn, of

$$\alpha^{\frac{\mu-1}{3}} \equiv 1$$

$$\beta^{\frac{\mu-1}{3}} \equiv f \pmod{p = \mu}.$$

$$\gamma^{\frac{\mu-1}{3}} \equiv f^2$$

Hieruit blijkt dus, dat de klassificatie der getallen

$$1, 2, 3, \dots, p-1$$

met behulp dezer drie laatste congruenties, samenvalt met die volgens hun cubisch karakter ten opzichte van den modulus  $a + b\varrho$ .

Het resultaat

$$\left[ \frac{3}{a + b\varrho} \right] = \varrho^{-\frac{1}{3}b}$$

kan nu aldus uitgesproken worden: het getal 3 behoort tot de klasse A, B of C, al naar dat  $-\frac{1}{3}b$  van den vorm  $3m$ ,  $3m+1$  of  $3m+2$  is.

Ik laat hier eenige voorbeelden volgen.

$$p=7, \quad a=2, \quad b=3, \quad f=4.$$

Schema S

A 1, 6.

$h \ j \ k$  0 1

B 2, 5.

$j \ k \ l$  1 0

C 3, 4.

$k \ l \ j$  0 1

$$p=13, \quad a=-1, \quad b=3, \quad f=9.$$

A 1, 5, 8, 12.

0 2

B 4, 6, 7, 9.

2 1

C 2, 3, 10, 11.

1 1

1, 7, 8, 11, 12, 18.	2 2
4, 6, 9, 10, 13, 15.	2 1
2, 3, 5, 14, 16, 17.	1 3

$$p=31, \quad a=5, \quad b=6, \quad f=25.$$

1, 2, 4, 8, 15, 16, 23, 27, 29, 30.	3 4
3, 6, 7, 12, 14, 17, 19, 24, 25, 28.	4 2
5, 9, 10, 11, 13, 18, 20, 21, 22, 26.	2 4

$$p=37, \quad a=-4, \quad b=3, \quad f=26.$$

1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36.	2 5
2, 9, 12, 15, 16, 17, 20, 21, 22, 25, 28, 35.	5 4
3, 4, 5, 7, 13, 18, 19, 24, 30, 32, 33, 34.	4 3

$$p=43, \quad a=-1, \quad b=6, \quad f=36.$$

1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42.	3 6
3, 5, 6, 10, 12, 19, 20, 23, 24, 31, 33, 37, 38, 40.	6 4
7, 9, 13, 14, 15, 17, 18, 25, 26, 28, 29, 30, 34, 36.	4 4

$$p=61, \quad a=5, \quad b=9, \quad f=13.$$

1, 3, 8, 9, 11, 20, 23, 24, 27, 28, 33, 34, 37,	6 8
38, 41, 50, 52, 53, 58, 60.	8 5
4, 10, 12, 14, 17, 19, 25, 26, 29, 30, 31, 32, 35,	5 7
36, 42, 44, 47, 49, 51, 57.	
2, 5, 6, 7, 13, 15, 16, 18, 21, 22, 39, 40, 43,	
45, 46, 48, 54, 55, 56, 59.	

Terwijl over het voorkomen van het getal 3 in de groepen A, B, op bovenstaande wijze vooruit beslist is, kan men nu, met behulp van de reciprociteitswet, in de theorie der cubische resten gemakkelijk de kenmerken opstellen, noodig om het voorkomen ook van andere getallen in deze klassen te onderkennen. Het is hierbij voldoende om alleen priemgetallen te beschouwen.

Wat het priemgetal 2 betreft, kan men deze criteria, zonder hulp der reciprociteitswet, aldus afleiden.

31. Daar het getal  $p-1$  altijd tot A behoort, zoo volgt onmiddellijk, dat 2 tot de klasse A, B of C zal behooren al naar gelang

$\frac{p-1}{2}$  tot de klasse A, C of B behoort.



der congruenties

$$\begin{aligned} \alpha + \alpha' + 1 &\equiv 0 \\ \beta + \beta' + 1 &\equiv 0 \pmod{p}, \\ \gamma + \gamma' + 1 &\equiv 0 \end{aligned}$$

en daar men  $\alpha$  met  $\alpha'$ ,  $\beta$  met  $\beta'$ ,  $\gamma$  met  $\gamma'$  mag verwisselen, zijn deze drie aantallen even, uitgezonderd het eerste, wanneer  $\alpha = \alpha' = \frac{p-1}{2}$  tot A behoort, of uitgezonderd het tweede, wanneer  $\beta = \beta' = \frac{p-1}{2}$  tot B behoort, of uitgezonderd het derde, wanneer  $\gamma = \gamma' = \frac{p-1}{2}$  tot C behoort.

Hieruit blijkt dus, dat 2 tot de klasse A, B of C behoort, al naar dat van de drie getallen  $h, j, k$  het eerste, tweede of derde oneven is.

Daar  $p = 3n + 1$  ( $n$  even) en volgens art. 28

$$\begin{aligned} 9h &= 3n + 2a - b - 7, \\ 9j &= 3n - a + 2b - 1, \\ 9k &= 3n - a - b - 1 \end{aligned}$$

is, zoo is  $h$  oneven, wanneer  $b$  even is,  $j$  oneven, wanneer  $a$  even is, eindelijk  $k$  oneven, wanneer  $a$  en  $b$  beide oneven zijn. Daar  $a$  en  $b$  geen gemeenen deeler hebben, zoo zijn geen andere gevallen mogelijk, dus 2 behoort tot

$$\begin{aligned} \text{A,} & \text{wanneer } b \equiv 0 \\ \text{B,} & \text{" } a \equiv 0 \pmod{2}. \\ \text{C,} & \text{" } a \equiv b \equiv 1 \end{aligned}$$

32. Wat het voorkomen van 5 betreft, volgens de cubische reciprociteitswet is

$$\left[ \frac{5}{a + b\varrho} \right] = \left[ \frac{a + b\varrho}{5} \right],$$

want 5 is ook in de theorie der geheele getallen  $a + b\varrho$  een priemgetal.

Voor  $a \equiv 0 \pmod{5}$  is dus

$$\left[ \frac{5}{a + b\varrho} \right] = \left[ \frac{b\varrho}{5} \right] = \left[ \frac{\varrho}{5} \right] = \varrho^8 = \varrho^2;$$

derhalve behoort 5 tot C.

Is  $a$  niet door 5 deelbaar, dan kan men  $x$  bepalen uit

$$b \equiv ax \pmod{5},$$

en  $x$  kan de waarden 0, 1, 2, 3, 4 aannemen; men heeft also

$$\left[ \frac{5}{a + b\varrho} \right] = \left[ \frac{a(1 + x\varrho)}{5} \right] = \left[ \frac{1 + x\varrho}{5} \right]$$

en men vindt voor

$$x = 0 \quad \left[ \frac{5}{a + b\varrho} \right] = 1,$$

$$x = 1 \quad \left[ \frac{5}{a + b\varrho} \right] = \varrho,$$

$$x = 2 \quad \left[ \frac{5}{a + b\varrho} \right] = 1,$$

$$x = 3 \quad \left[ \frac{5}{a + b\varrho} \right] = \varrho^2,$$

$$x = 4 \quad \left[ \frac{5}{a + b\varrho} \right] = \varrho.$$

Hieruit volgt, dat 5 behoort tot

$$\text{A, wanneer } b \equiv 0, \quad b \equiv 2a$$

$$\text{B, } \quad \quad b \equiv a, \quad b \equiv 4a \pmod{5}.$$

$$\text{C, } \quad \quad b \equiv 3a, \quad a \equiv 0.$$

Om het voorkomen van 7 te beoordeelen, heeft men

$$\left[ \frac{7}{a + b\varrho} \right] = \left[ \frac{2 + 3\varrho}{a + b\varrho} \right] \left[ \frac{2 + 3\varrho^2}{a + b\varrho} \right]$$

en nu volgens de reciprociteitswet

$$\left[ \frac{7}{a + b\varrho} \right] = \left[ \frac{a + b\varrho}{2 + 3\varrho} \right] \left[ \frac{a + b\varrho}{2 + 3\varrho^2} \right].$$

Voor  $a \equiv 0 \pmod{7}$  volgt, daar in 't algemeen

$$\left[ \frac{a + \beta\varrho}{a + b\varrho} \right] \left[ \frac{a + \beta\varrho^2}{a + b\varrho^2} \right] = 1$$

is,

$$\left[ \frac{7}{a + b\varrho} \right] = \left[ \frac{\varrho}{2 + 3\varrho} \right] \left[ \frac{\varrho}{2 + 3\varrho^2} \right] = \left[ \frac{\varrho^2}{2 + 3\varrho^2} \right] = \varrho^4 = \varrho,$$

zoodat 7 tot B behoort.

Is  $a$  niet door 7 deelbaar, maar

dan volgt

$$\left[ \frac{7}{a + b\varrho} \right] = \left[ \frac{1 + x\varrho}{2 + 3\varrho} \right] \left[ \frac{1 + x\varrho}{2 + 3\varrho^2} \right],$$

en voor  $x$  kunnen de waarden

$$0, 1, 2, 4, 6$$

voorkomen, niet  $x=3$  en  $x=5$ , daar deze waarden

$$p = a^2 - ab + b^2 \equiv a^2 (1 - x + x^2)$$

door 7 deelbaar zouden maken.

Men vindt nu voor

$$x=0 \quad \left[ \frac{7}{a + b\varrho} \right] = 1,$$

$$x=1 \quad \left[ \frac{7}{a + b\varrho} \right] = \varrho^2,$$

$$x=2 \quad \left[ \frac{7}{a + b\varrho} \right] = 1,$$

$$x=4 \quad \left[ \frac{7}{a + b\varrho} \right] = \varrho,$$

$$x=6 \quad \left[ \frac{7}{a + b\varrho} \right] = \varrho^2,$$

zoodat 7 behoort tot

A, wanneer  $b \equiv 0$ ,  $b \equiv 2a$

B, „  $b \equiv 4a$ ,  $a \equiv 0 \pmod{7}$ .

C, „  $b \equiv a$ ,  $b \equiv 6a$

Op gelijke wijze, of door inductie, zal men vinden dat

11 behoort tot

A voor  $b \equiv 0$ ,  $b \equiv 2a$ ,  $b \equiv 4a$ ,  $b \equiv 5a$

B „  $b \equiv 3a$ ,  $b \equiv 6a$ ,  $b \equiv 9a$ ,  $a \equiv 0 \pmod{11}$ ,

C „  $b \equiv a$ ,  $b \equiv 7a$ ,  $b \equiv 8a$ ,  $b \equiv 10a$

13 behoort tot

A voor  $b \equiv 0$ ,  $b \equiv 2a$ ,  $b \equiv 3a$ ,  $b \equiv 8a$

B „  $b \equiv a$ ,  $b \equiv 6a$ ,  $b \equiv 11a$ ,  $b \equiv 12a \pmod{13}$ ,

C „  $b \equiv 5a$ ,  $b \equiv 7a$ ,  $b \equiv 9a$ ,  $a \equiv 0$

19 behoort tot

(mod 19),

A voor  $b \equiv 0$ ,  $b \equiv a$ ,  $b \equiv 2a$ ,  $b \equiv 10a$ ,  $b \equiv 18a$ ,  $a \equiv 0$   
 B „  $b \equiv 5a$ ,  $b \equiv 11a$ ,  $b \equiv 13a$ ,  $b \equiv 14a$ ,  $b \equiv 16a$ ,  $b \equiv 17a$   
 C „  $b \equiv 3a$ ,  $b \equiv 4a$ ,  $b \equiv 6a$ ,  $b \equiv 7a$ ,  $b \equiv 9a$ ,  $b \equiv 15a$

23 behoort tot

(mod 23),

A voor  $b \equiv 0$ ,  $b \equiv 2a$ ,  $b \equiv 5a$ ,  $b \equiv 6a$ ,  $b \equiv 7a$ ,  $b \equiv 8a$ ,  $b \equiv 11a$ ,  $b \equiv 15a$   
 B „  $b \equiv a$ ,  $b \equiv 9a$ ,  $b \equiv 13a$ ,  $b \equiv 16a$ ,  $b \equiv 17a$ ,  $b \equiv 18a$ ,  $b \equiv 19a$ ,  $b \equiv 22a$   
 C „  $b \equiv 3a$ ,  $b \equiv 4a$ ,  $b \equiv 10a$ ,  $b \equiv 12a$ ,  $b \equiv 14a$ ,  $b \equiv 20a$ ,  $b \equiv 21a$ ,  $a \equiv 0$ .

33. De beschouwing van deze bijzondere theorema's geeft aanleiding tot de volgende opmerkingen.

Voor het gemak zal ik in het volgende de reële priemgetallen van den vorm  $3n - 1$ , die ook in de complexe theorie priemgetallen blijven door Q, de priemgetallen van den vorm  $3n + 1$  door P aanduiden.

1. Een priemgetal Q behoort, wanneer  $a \equiv 0 \pmod{Q}$ , tot de klassen

A, B, C al naar dat  $\frac{Q+1}{3}$  van den vorm  $3m$ ,  $3m+1$ ,  $3m+2$  is.

2. Een priemgetal P behoort, wanneer  $a \equiv 0 \pmod{P}$ , tot de klassen

A, B, C al naar dat  $\frac{P-1}{6}$  van den vorm  $3m$ ,  $3m+1$ ,  $3m+2$  is.

3. In de gevallen  $b \equiv 0$ ,  $b \equiv 2a$  behoort het priemgetal P of Q altijd tot de klasse A.

4. Behoort het priemgetal tot A voor  $a \equiv 0$ , dan behoort het ook tot A voor  $b \equiv a$  en voor  $b \equiv -a$ . Komt het priemgetal echter in de klasse B of C voor, wanneer  $a \equiv 0$ , dan komt het voor  $b \equiv a$  en voor  $b \equiv -a$  in de klasse C of B voor.

5. In het algemeen zijn de criteria van den navolgenden vorm. Is  $a \equiv 0$ , dan behoort het priemgetal tot eene bepaalde klasse.

Is  $a$  niet  $\equiv 0$ , dan is  $b \equiv ax$  en voor elke waarde van  $x$  behoort het priemgetal in eene bepaalde klasse, zoodat men de waarden van  $x$  in 3 groepen  $\alpha$ ,  $\beta$ ,  $\gamma$  kan onderscheiden, zoodanig dat voor

$b \equiv a\alpha$  het priemgetal tot A,

$b \equiv a\beta$  „ „ „ B,

$b \equiv a\gamma$  „ „ „ C,

klasse correspondeert.

Het totale aantal der congruenties nu, die men op deze wijze voor elk der drie klassen vindt, is even groot en gelijk aan  $\frac{Q+1}{3}$  of aan  $\frac{P-1}{3}$ .

6. Zijn  $x$  en  $y$  twee getallen, die voldoen aan de congruentie

$$x + y - xy \equiv 0,$$

dan behoort  $x$  tot  $\alpha$ , dan behoort ook  $y$  tot  $\alpha$ . Is echter  $x = \beta$  of  $x = \gamma$ , dan behoort  $y$  respectievelijk tot de  $\gamma$ 's of de  $\beta$ 's.

Is  $xy \equiv 1$  en behoort 1 tot de  $\alpha$ 's, dan is

$$\text{voor } x = \alpha' \quad y = \alpha'',$$

$$\text{voor } x = \beta' \quad y = \gamma',$$

$$\text{voor } x = \gamma' \quad y = \beta'.$$

Is  $xy \equiv 1$  en  $1 = \beta$ , dan is

$$\text{voor } x = \alpha \quad y = \gamma,$$

$$\text{voor } x = \beta' \quad y = \beta'',$$

$$\text{voor } x = \gamma' \quad y = \alpha'.$$

Is  $xy \equiv 1$  en  $1 = \gamma$ , dan is

$$\text{voor } x = \alpha \quad y = \beta,$$

$$\text{voor } x = \beta \quad y = \alpha,$$

$$\text{voor } x = \gamma \quad y = \gamma'.$$

34. Wat het bewijs van de bovenstaande opmerkingen betreft, alleen het onder 5 gezegde vereischt eenige nieuwe beschouwingen, al het overige levert na het voorafgaande geen moeilijkheden op. Ik ga er dan nu toe over het onder 5 opgemerkte algemeen aan te toonen. Hierbij zijn de gevallen, dat het priemgetal gelijk aan  $Q$  of aan  $P$  is, afzonderlijk te behandelen, en wel zal eerst het eerste geval (verreweg het eenvoudigste) beschouwd worden.

35. Is dan het priemgetal  $Q$  van den vorm  $3n-1$ , dus ook priem in de theorie der complexe getallen van den vorm  $a + b\varrho$ , dan is volgens de wet van reciprociteit

$$\left[ \frac{Q}{a + b\varrho} \right] = \left[ \frac{a + b\varrho}{Q} \right].$$

$$\left[ \frac{Q}{a + b\varrho} \right] = \left[ \frac{b\varrho}{Q} \right] = \left[ \frac{\varrho}{Q} \right] = \varrho^{\frac{Q^2-1}{3}}.$$

Nu is

$$\frac{Q+1}{3} \times (Q-2)$$

een veelvoud van 3 en

$$\frac{Q^2-1}{3} - \frac{(Q+1)(Q-2)}{3} = \frac{Q+1}{3},$$

derhalve is voor  $a \equiv 0 \pmod{Q}$

$$\left[ \frac{Q}{a + b\varrho} \right] = \varrho^{\frac{Q+1}{3}},$$

waarmede de juistheid van het in art. 33 onder 1 gezegde aangetoond is.

Is  $a$  niet door  $Q$  deelbaar, dan is  $x$  volkomen bepaald door

$$b \equiv ax \pmod{Q}$$

en men heeft

$$\left[ \frac{Q}{a + b\varrho} \right] = \left[ \frac{a(1+x\varrho)}{Q} \right] = \left[ \frac{1+x\varrho}{Q} \right],$$

waaruit reeds blijkt, dat de klasse, waartoe  $Q$  behoort, alleen van het getal  $x$  afhangt, terwijl voor  $x$  blijkbaar de getallen

$$0, 1, 2, 3, \dots, Q-1$$

kunnen voorkomen.

Wij hebben nu nog slechts deze vraag te beantwoorden: hoeveel der  $Q$  grootheden

$$\left[ \frac{1+x\varrho}{Q} \right]$$

$$(x=0, 1, 2, 3, \dots, Q-1)$$

zijn gelijk aan 1, hoeveel gelijk aan  $\varrho$ , hoeveel gelijk aan  $\varrho^2$ ? Wij beschouwen een volledig systeem niet door den modulus deelbare getallen, voor hetwelk de getallen

$$\alpha + \beta\varrho$$

$$\left( \begin{matrix} \alpha \\ \beta \end{matrix} = 0, 1, 2, 3, \dots, Q-1 \right)$$

genomen kunnen worden, waarbij alleen de combinatie  $\alpha = 0, \beta = 0$

te laten is. Brengen wij deze  $Q$  getallen naar een karakter tot 3 groepen A, B, C,

$$\begin{array}{ll} A & a_0 + \beta_0 \varrho, \dots \\ B & a_1 + \beta_1 \varrho, \dots \\ C & a_2 + \beta_2 \varrho, \dots \end{array}$$

dan bevat elk dezer groepen

$$\frac{Q^2 - 1}{3} = (Q - 1) \times \frac{Q + 1}{3}$$

getallen, welk aantal dus een veelvoud van  $Q - 1$  is; en de reële getallen

$$1, 2, 3, \dots, Q - 1,$$

die met  $\beta = 0$  correspondeeren, behooren alle tot A, waaruit voortvloeit, dat zoo  $a + \beta \varrho$  tot zekere klasse behoort, ook de met

$$1(a + \beta \varrho), 2(a + \beta \varrho), \dots, (Q - 1)(a + \beta \varrho)$$

congruente getallen tot dezelfde klasse behooren. Is nu  $a$  niet gelijk nul, dan zijn

$$a, 2a, 3a, \dots, (Q - 1)a$$

volgens den modulus  $Q$  in zekere volgorde congruent met

$$1, 2, 3, \dots, Q - 1.$$

Men kan dus de getallen van een klasse, waarbij het reële deel niet gelijk nul is, in groepen van  $Q - 1$  getallen verdeelen, zoodat in elke groep één getal voorkomt van den vorm  $1 + x \varrho$ .

Hieruit blijkt dus, dat de aantallen der getallen  $1 + x \varrho$ , die  $\left[ \frac{1 + x \varrho}{Q} \right]$  gelijk aan 1,  $\varrho$  of  $\varrho^2$  maken, zijn

$$\frac{Q - 2}{3}, \quad \frac{Q + 1}{3}, \quad \frac{Q + 1}{3}, \quad \text{wanneer} \left[ \frac{\varrho}{Q} \right] = 1,$$

$$\frac{Q + 1}{3}, \quad \frac{Q - 2}{3}, \quad \frac{Q + 1}{3}, \quad \text{wanneer} \left[ \frac{\varrho}{Q} \right] = \varrho,$$

$$\frac{Q + 1}{3}, \quad \frac{Q + 1}{3}, \quad \frac{Q - 2}{3}, \quad \text{wanneer} \left[ \frac{\varrho}{Q} \right] = \varrho^2$$

is, en daar verder boven gevonden werd, dat voor

$$a \equiv 0 \pmod{Q}$$

$a$  tot de klassen A, B of C behoort al naar dat  $\left[ \frac{\varrho}{Q} \right]$  gelijk aan 1,  $\varrho$  of  $\varrho^2$

voor het geval, dat het priemgetal van den vorm  $3n - 1$  is.

36. Is het priemgetal, waarvan men het voorkomen in de klasse A, B, C wil onderzoeken, van den vorm  $P = 3n + 1$ , dan komt het er dus op aan de waarde van

$$\left[ \frac{P}{a + b\varrho} \right]$$

te bepalen; daar  $P$  geen priemgetal is in de complexe theorie, zoo is het in de eerste plaats noodig, vóórdat de wet van reciprociteit toegepast kan worden,  $P$  in zijne primaire priemfactoren te ontbinden.

Stel

$$P = (A + B\varrho)(A + B\varrho^2),$$

dan is volgens de reciprociteitswet

$$\left[ \frac{P}{a + b\varrho} \right] = \left[ \frac{a + b\varrho}{A + B\varrho} \right] \left[ \frac{a + b\varrho}{A + B\varrho^2} \right].$$

Dus heeft men

$$\text{voor } a \equiv 0 \pmod{P}$$

$$\left[ \frac{P}{a + b\varrho} \right] = \left[ \frac{\varrho}{A + B\varrho} \right] \left[ \frac{\varrho}{A + B\varrho^2} \right] = \varrho^{\frac{2(P-1)}{3}} = \varrho^{\frac{P-1}{6}},$$

$$\text{voor } ax \equiv b \pmod{P}$$

$$\left[ \frac{P}{a + b\varrho} \right] = \left[ \frac{1 + x\varrho}{A + B\varrho} \right] \left[ \frac{1 + x\varrho}{A + B\varrho^2} \right].$$

Uit de eerste uitkomst voor  $a \equiv 0$  blijkt de juistheid van de tweede bewering in art. 33.

Daar  $P$  van den vorm  $3n + 1$  is, zoo heeft de congruentie

$$x^3 \equiv 1 \pmod{P}$$

drie verschillende wortels,  $1, f, g$ , waarbij  $f \equiv g^2$ .

De beide waarden  $-f, -g$  kunnen nu niet gelijk aan  $x$  zijn in de congruentie

$$b \equiv ax,$$

want uit  $b \equiv -af$  zoude volgen

$$a^2 - ab + b^2 \equiv a^2(1 + f + f^2) \equiv 0 \pmod{P},$$

oodat het priemgetal

$$p = a^2 - ab + b^2$$

door  $P$  deelbaar zou zijn.



$$0, 1, 2, 3, \dots, P-1$$

met weglating der beide getallen  $P-f$  en  $P-g$ . Hun aantal derhalve  $P-2$ , en nu is te onderzoeken, voor hoeveel dezer  $P$ -waarden van  $x$  de uitdrukking

$$\left[ \frac{1+x\varrho}{A+B\varrho} \right] \left[ \frac{1+x\varrho}{A+B\varrho^2} \right]$$

de waarden 1,  $\varrho$  en  $\varrho^2$  aanneemt.

Ik merk nog op, dat

$$\left[ \frac{\varrho}{A+B\varrho} \right] = \varrho^{\frac{P-1}{3}}$$

is en dat voor  $a \equiv 0 \pmod{P}$  geldt

$$\left[ \frac{P}{a+b\varrho} \right] = \varrho^{\frac{2(P-1)}{3}}.$$

Behoort dus  $\varrho$  voor den modulus  $A+B\varrho$  tot de klasse A, B of C, dan behoort gelijktijdig  $P$  voor den modulus  $a+b\varrho$  (of wat hetzelfde is, voor den reëlen modulus  $p$ ) tot de klasse A, C of B.

37. Men kan steeds, wanneer een willekeurig getal  $\alpha + \beta\varrho$  gegeven is, een daarmede volgens den modulus  $A+B\varrho$  congruent getal vinden, waarvan het reële deel gelijk aan 1 is.

De verdeeling van een volledig systeem niet door den modulus deelbare getallen in drie klassen, volgens hun cubisch karakter kan dus aldus voorgesteld worden

$$(\text{mod } A+B\varrho)$$

A	$\alpha = 1 + a\varrho,$	$\alpha' = 1 + a'\varrho,$	$\alpha'' = 1 + a''\varrho, \dots$
B	$\beta = 1 + b\varrho,$	$\beta' = 1 + b'\varrho,$	$\beta'' = 1 + b''\varrho, \dots$
C	$\gamma = 1 + c\varrho,$	$\gamma' = 1 + c'\varrho,$	$\gamma'' = 1 + c''\varrho, \dots$

en daar uit

$$(1+a\varrho)^{\frac{P-1}{3}} - \varrho^k \equiv (A+B\varrho)(C+D\varrho)$$

volgt

$$(1+a\varrho^2)^{\frac{P-1}{3}} - \varrho^{2k} \equiv (A+B\varrho^2)(C+D\varrho^2),$$

voorgesteld worden

$$\begin{array}{lll}
 & & (\text{mod } A + B \varrho^2) \\
 A & 1 + a \varrho^2, & 1 + a' \varrho^2, & 1 + a'' \varrho^2, \dots \\
 B & 1 + c \varrho^2, & 1 + c' \varrho^2, & 1 + c'' \varrho^2, \dots \\
 C & 1 + b \varrho^2, & 1 + b' \varrho^2, & 1 + b'' \varrho^2, \dots
 \end{array}$$

De getallen  $a, b, c, a', b', c', a'', b'', c'', \dots$  vormen in hun geheel alle getallen van de groep

$$0, 1, 2, 3, \dots, P-1,$$

met uitzondering van het enkele getal, dat  $\equiv -\varrho^2 \pmod{A + B \varrho}$  is en dat  $\pmod{P}$  congruent is met een der getallen  $-f, -g$ . De gevallen nu, dat

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = 1$$

is, zijn blijkbaar deze

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = 1 \text{ en te gelijker tijd } \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = 1,$$

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = \varrho \text{ en te gelijker tijd } \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = \varrho^2,$$

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = \varrho^2 \text{ en te gelijker tijd } \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = \varrho.$$

Nu is  $\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = 1$  voor  $x = a, a', a'', \dots$ , en zal nu te gelijker tijd  $\left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = 1$  zijn, dan moet dus  $1 + a \varrho$  volgens den modulus  $A + B \varrho^2$  congruent zijn met een der getallen  $1 + a \varrho^2, 1 + a' \varrho^2, \dots$  dus is te stellen

$$1 + a \varrho \equiv 1 + a' \varrho^2 \pmod{A + B \varrho^2}.$$

Omgekeerd, zoo aan deze congruentie voldaan is, heeft men

$$\left[ \frac{1 + a \varrho}{A + B \varrho} \right] = 1, \quad \left[ \frac{1 + a \varrho}{A + B \varrho^2} \right] = 1.$$

Het aantal malen, dat dit geval zich dus voordoet, is gelijk aan het aantal oplossingen van bovenstaande congruentie. Op soortgelijke wijze voor de beide overige gevallen

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = \varrho, \quad \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = \varrho^2$$

$$\left[ \frac{1+x\varrho}{A+B\varrho} \right] = \varrho^2, \quad \left[ \frac{1+x\varrho}{A+B\varrho^2} \right] = \varrho$$

redeneerende, volgt dat het geheele aantal malen, dat de uitdrukking

$$\left[ \frac{1+x\varrho}{A+A\varrho} \right] \left[ \frac{1+x\varrho}{A+B\varrho^2} \right]$$

gelijk 1 is, voorgesteld wordt door de som van het aantal oplossingen der drie congruenties

$$\begin{aligned} 1+a\varrho &\equiv 1+a'\varrho^2 \\ 1+b\varrho &\equiv 1+b'\varrho^2 \pmod{A+B\varrho^2}. \\ 1+c\varrho &\equiv 1+c'\varrho^2 \end{aligned}$$

Evenzoo blijkt, dat het aantal malen, dat bovenstaande uitdrukking gelijk aan  $\varrho$  of aan  $\varrho^2$  wordt, uitgedrukt wordt, in het eerste geval door de som van het aantal oplossingen der congruenties

$$\begin{aligned} 1+b\varrho &\equiv 1+a\varrho^2 \\ 1+c\varrho &\equiv 1+b\varrho^2 \pmod{A+B\varrho^2}, \\ 1+a\varrho &\equiv 1+c\varrho^2 \end{aligned}$$

en in het tweede geval door de som van het aantal oplossingen der congruenties

$$\begin{aligned} 1+c\varrho &\equiv 1+a\varrho^2 \\ 1+a\varrho &\equiv 1+b\varrho^2 \pmod{A+B\varrho^2}. \\ 1+b\varrho &\equiv 1+c\varrho^2 \end{aligned}$$

Om onmiddellijk de ontwikkelingen van art. 25—28 te kunnen toepassen, is het iets gemakkelijker alleen congruenties voor den modulus  $A+B\varrho$  te beschouwen, zoodat wij, in de voorgaande formules overal  $\varrho$  door  $\varrho^2$  vervangende, zullen schrijven, wanneer  $t, u, v$  de aantallen malen zijn, dat

$$\left[ \frac{1+x\varrho}{A+B\varrho} \right] \times \left[ \frac{1+x\varrho}{A+B\varrho^2} \right]$$

respectievelijk gelijk aan 1,  $\varrho$  of  $\varrho^2$  is:

=som aantal oplossingen van

$$\begin{aligned} 1+a\varrho^2 &\equiv 1+a'\varrho \\ 1+b\varrho^2 &\equiv 1+b'\varrho \pmod{A+B\varrho}, \\ 1+c\varrho^2 &\equiv 1+c'\varrho \end{aligned}$$

= som aantal oplossingen van

$$\begin{aligned} 1 + b \varrho^2 &\equiv 1 + a \varrho \\ 1 + c \varrho^2 &\equiv 1 + b \varrho \pmod{A + B \varrho}, \\ 1 + a \varrho^2 &\equiv 1 + c \varrho \end{aligned}$$

$v$  = som aantal oplossingen van

$$\begin{aligned} 1 + c \varrho^2 &\equiv 1 + a \varrho \\ 1 + a \varrho^2 &\equiv 1 + b \varrho \pmod{A + B \varrho}, \\ 1 + b \varrho^2 &\equiv 1 + c \varrho \end{aligned}$$

38. Hierbij dient nog het volgende opgemerkt te worden. Onder de getallen  $a, b, c, a', b', c', \dots$  komt één der getallen  $-f, -g$  niet voor. Laten wij onderstellen, dat  $-f$  niet voorkomt, zoodat  $-g$  wel voorkomt. Dan is het toch duidelijk, dat niettemin deze waarde  $-f$  nergens in een der bovenstaande congruenties kan voorkomen, want bijv. uit  $1 + a \varrho^2 \equiv 1 + a' \varrho$  of  $a \varrho^2 \equiv a' \varrho$  zou voor  $a = -g$  volgen  $a' \equiv a \varrho \equiv -\varrho^2 \equiv -f$ , want  $f \equiv \varrho^2$  en  $g \equiv \varrho \pmod{A + B \varrho}$  en de waarde  $a' \equiv -f$  komt niet voor. Daar nu onder de voor  $x$  te nemen waarden  $a, b, c, a', b', c', \dots$  zoowel  $-f$  als  $-g$  niet voorkwamen, zoo is hierdoor klaar, dat werkelijk de bovenstaande uitdrukkingen voor  $t, u$  en  $v$  juist zijn, wanneer de in de congruenties voorkomende getallen  $a, a', b, b', c, c'$  of alle mogelijke wijzen uit de groepen  $a, a', a'', \dots, b, b', b'', \dots, c, c', c'', \dots$  gekozen worden.

Voeren wij nu in plaats van  $a, b$ , enz. liever de getallen  $\alpha = 1 + a \varrho, \beta = 1 + b \varrho$ , enz. in, dan gaat bijv.  $a \varrho^2 \equiv a' \varrho$  over in

$$\varrho(\alpha - 1) \equiv \alpha' - 1,$$

of in

$$\alpha' - \varrho \alpha \equiv 1 - \varrho$$

en, evenzoo met de overige congruenties handelende, vinden wij het volgende:

= som aantal oplossingen van

$$\begin{aligned} \alpha' - \varrho \alpha &\equiv 1 - \varrho \\ \beta' - \varrho \beta &\equiv 1 - \varrho \pmod{A + B \varrho}, \\ \alpha' &\equiv 1 - \varrho \end{aligned}$$

$$\begin{aligned} \alpha - \varrho \beta &\equiv 1 - \varrho \\ \beta - \varrho \gamma &\equiv 1 - \varrho \pmod{A + B \varrho}, \\ \gamma - \varrho \alpha &\equiv 1 - \varrho \end{aligned}$$

$v$  = som aantal oplossingen van

$$\begin{aligned} \alpha - \varrho \gamma &\equiv 1 - \varrho \\ \beta - \varrho \alpha &\equiv 1 - \varrho \pmod{A + B \varrho}, \\ \gamma - \varrho \beta &\equiv 1 - \varrho. \end{aligned}$$

In het eerste lid dezer congruenties kan het teeken — overal door + vervangen worden, daar twee getallen  $\lambda$  en  $-\lambda$  steeds tot dezelfde klasse behooren. Doen wij dit, en vermenigvuldigen wij bovendien met het geheele getal

$$\frac{P-1}{1-\varrho} = \frac{3n}{1-\varrho} = n(1-\varrho^2),$$

dan volgt:

$t$  = som aantal oplossingen van

$$\begin{aligned} \alpha' + \varrho \alpha + 1 &\equiv 0 \\ \beta' + \varrho \beta + 1 &\equiv 0 \pmod{A + B \varrho}, \\ \gamma' + \varrho \gamma + 1 &\equiv 0 \end{aligned}$$

$u$  = som aantal oplossingen van

$$\begin{aligned} \alpha + \varrho \beta + 1 &\equiv 0 \\ \beta + \varrho \gamma + 1 &\equiv 0 \pmod{A + B \varrho}, \\ \gamma + \varrho \alpha + 1 &\equiv 0 \end{aligned}$$

$v$  = som aantal oplossingen van

$$\begin{aligned} \alpha + \varrho \gamma + 1 &\equiv 0 \\ \beta + \varrho \alpha + 1 &\equiv 0 \pmod{A + B \varrho}, \\ \gamma + \varrho \beta + 1 &\equiv 0 \end{aligned}$$

en wel komt men tot dit besluit in elk der drie onderstellingen, die men kan maken, namelijk dat  $n(1-\varrho^2)$  tot de klasse A, B of C behoort. Dit is blijkbaar daaraan toe te schrijven, dat de bovenstaande groepen van 3 congruenties zoodanig zijn, dat zij bij eene cyclische verwisseling van  $\alpha, \beta, \gamma$  onveranderd blijven.

Er zijn nu drie gevallen te onderscheiden.

I.  $\varrho$  behoort tot A, zoodat  $\left[ \frac{\varrho}{A + B \varrho} \right] = 1$ .

de sommen der aantallen oplossingen van de volgende congruenties

$u$	$v$	$w$
$\alpha + \alpha' + 1 \equiv 0,$	$\alpha + \beta + 1 \equiv 0,$	$\alpha + \gamma + 1 \equiv 0,$
$\beta + \beta' + 1 \equiv 0,$	$\beta + \gamma + 1 \equiv 0,$	$\beta + \alpha + 1 \equiv 0,$
$\gamma + \gamma' + 1 \equiv 0,$	$\gamma + \alpha + 1 \equiv 0,$	$\gamma + \beta + 1 \equiv 0,$

er komt volgens art. 25, wanneer wij de daar voor het priemgetal  $A + Bq$  gevonden resultaten overdragen op den modulus  $A + Bq$  met de norm  $3n + 1$ ,

$$\begin{aligned} u &= h + k + j = n - 1, \\ v &= j + l + k = n, \\ w &= k + j + l = n. \end{aligned}$$

Volgens art. 36 is in dit geval voor  $\alpha \equiv 0$ ,  $\left[ \frac{P}{\alpha + bq} \right] = 1$ .

II.  $q$  behoort tot B, zoodat  $\left[ \frac{q}{A + Bq} \right] = q$ .

Dan zijn  $u, v, w$  de sommen der aantallen oplossingen van de volgende congruenties

$u$	$v$	$w$
$\alpha + \beta + 1 \equiv 0,$	$\alpha + \gamma + 1 \equiv 0,$	$\alpha + \alpha' + 1 \equiv 0,$
$\beta + \gamma + 1 \equiv 0,$	$\beta + \alpha + 1 \equiv 0,$	$\beta + \beta' + 1 \equiv 0,$
$\gamma + \alpha + 1 \equiv 0,$	$\gamma + \beta + 1 \equiv 0,$	$\gamma + \gamma' + 1 \equiv 0,$

er volgt

$$\begin{aligned} u &= n \\ v &= n \\ w &= n - 1. \end{aligned}$$

Volgens art. 36 is in dit geval voor  $\alpha \equiv 0$ ,  $\left[ \frac{P}{\alpha + bq} \right] = q^2$ .

III.  $q$  behoort tot C, zoodat  $\left[ \frac{q}{A + Bq} \right] = q^2$ .

In dit geval zijn  $u, v, w$  de sommen der aantallen oplossingen van

$u$	$v$	$w$
$\alpha + \gamma + 1 \equiv 0,$	$\alpha + \alpha' + 1 \equiv 0,$	$\alpha + \beta + 1 \equiv 0,$
$\beta + \alpha + 1 \equiv 0,$	$\beta + \beta' + 1 \equiv 0,$	$\beta + \gamma + 1 \equiv 0,$
$\gamma + \beta + 1 \equiv 0,$	$\gamma + \gamma' + 1 \equiv 0,$	$\gamma + \alpha + 1 \equiv 0,$

$$\begin{aligned}u &= n, \\v &= n - 1, \\w &= n.\end{aligned}$$

Volgens art. 36 is hier voor  $a \equiv 0$ ,  $\left[ \frac{P}{a + b\varrho} \right] = \varrho$ .

Hiermede is nu alles bewezen, wat in art. 33 gezegd is omtrent den algemeenen vorm der criteria, waaraan men het voorkomen van een priemgetal in de drie klassen kan onderkennen.

39. Wat de overige opmerkingen in art. 33 betreft, bedenken men, dat het onder 6 voorkomende onmiddellijk volgt uit de beide formules

$$\begin{aligned}\left[ \frac{1 + x\varrho}{Q} \right] \left[ \frac{1 + y\varrho}{Q} \right] &= \left[ \frac{1 - xy + (x + y - xy)\varrho}{Q} \right], \\ \left[ \frac{1 + x\varrho}{A + B\varrho} \right] \left[ \frac{1 + x\varrho}{A + B\varrho^2} \right] \left[ \frac{1 + y\varrho}{A + B\varrho} \right] \left[ \frac{1 + y\varrho}{A + B\varrho^2} \right] &= \\ &= \left[ \frac{1 - xy + (x + y - xy)\varrho}{A + B\varrho} \right] \left[ \frac{1 - xy + (x + y - xy)\varrho}{A + B\varrho^2} \right].\end{aligned}$$

Uit de opmerking, dat voor  $b \equiv 2a$  het priemgetal  $(2, 5, 7, 11, \dots)$  steeds tot de klasse A behoort, kan nog eene gevolgtrekking opge maakt worden, die het goed schijnt hier te plaatsén. Daar namelijk wegens

$$4p = 4(a^2 - ab + b^2) = (2a - b)^2 + 3b^2$$

3 niet tot de priemfactoren van  $2a - b$  behoort, zoo volgt, dat alle priemfactoren van  $2a - b$  cubische resten van  $p$  zijn en derhalve is  $2a - b$  zelf cubische rest van  $p$ .

40. Tot ditzelfde resultaat voert ook de volgende geheel verschillende beschouwing

Zij  $p = 3n + 1$  en laat  $z$  een volledig systeem congruente, niet door den modulus  $a + b\varrho$  deelbare getallen doorloopen, dan volgt uit

$$(z^3 + 1)^{2n} = z^{6n} + \dots + \frac{2n(2n-1)\dots(n+1)}{1. 2. 3. \dots n} z^{3n} + \dots + 1$$

de congruentie

$$\Sigma (z^3 + 1)^{2n} \equiv -2 - \frac{2n(2n-1)\dots(n+1)}{1. 2. 3. \dots n} \pmod{a + b\varrho}.$$

Maar aan den anderen kant vormen de getallen  $z^3, \dots$  alle cubische resten van  $a + b\varrho$ , elke rest 3 maal geschreven, en van de getallen  $z^3 + 1$  behooren er dus  $3h$  tot de klasse A,  $3j$  tot B,  $3k$  tot C, derhalve is ook

$$\Sigma (z^3 + 1)^{2n} \equiv 3h + 3k\varrho + 3j\varrho^2 \pmod{a + b\varrho},$$

of volgens de waarden van art. 28

$$\Sigma (z^3 + 1)^{2n} \equiv a - b - 2 - b \pmod{p},$$

plus is

$$-\frac{2n(2n-1)\dots(n+1)}{1\cdot 2\cdot 3\cdot\dots n}\equiv a-b-b\varrho\equiv 2a-b\pmod{a+b\varrho},$$

goedat ook

$$2a - b \equiv -\frac{2n(2n-1)\dots(n+1)}{1.2.3.\dots n} \pmod{p=3n+1}$$

s, welke merkwaardige congruentie het eerst door Jacobi in Crelle's Journal, Bd. 2 gegeven werd, en waarvan het bewijs gewoonlijk uit de formules afgeleid wordt, die in de theorie der cirkelverdeeling voorkomen.

Schrijft men deze congruentie aldus

$$(1 \cdot 2 \cdot 3 \cdot \dots \cdot n)^2 (2a - b) \equiv -1 \cdot 2 \cdot 3 \cdot \dots \cdot (2n) \pmod{p},$$

en bedenkt dat

$$\begin{array}{rcl} 2n+1 & \equiv & -n, \\ 2n+2 & \equiv & -(n-1), \\ 2n+3 & \equiv & -(n-2), \\ . & . & . \\ & 3n & \equiv -1, \end{array}$$

terwijl  $n$  even en  $1. 2. 3. \dots (3n) \equiv -1$  is, zoo volgt

$$(1 \cdot 2 \cdot 3 \cdot \dots \cdot n)^3 (2a - b) \equiv 1 \pmod{p},$$

waaruit onmiddellijk blijkt, dat  $2a - b$  cubische rest van  $p$  is, zooa  
 reeds boven op geheel andere wijze werd aangetoond. Uit dit eers  
 bewijs bleek bovendien, dat alle deeler van  $2a - b$  cubische reste  
 zijn.



## X.

(Haarlem, Arch. Néerl. Sci. Soc. Holl., 18, 1883, 358—436.)

(traduction autorisée par l'auteur)

---

### Contribution à la théorie des résidus cubiques et biquadratiques

Le théorème fondamental de la théorie des résidus quadratiques, la loi dite de réciprocité, est relatif au rapport réciproque de deux nombres premiers impairs, et dans une théorie complète le caractère du nombre 2, comme résidu ou non-résidu quadratique d'un autre nombre premier impair, doit donc être déterminé séparément. Il ressort de là que le nombre 2 occupe une place à part parmi tous les nombres premiers.

Les théorèmes par lesquels est déterminé le caractère de 2 ont été énoncés pour la première fois par Fermat<sup>1)</sup> et démontrés par Lagrange<sup>2)</sup>. Il convient de remarquer toutefois, que la démonstration de Lagrange s'appuie sur des considérations tout à fait semblables à celles par lesquelles, antérieurement, Euler<sup>3)</sup> avait démontré les théorèmes, également énoncés par Fermat, qui fixent le caractère de 3 comme résidu ou non-résidu quadratique. L'insuccès d'Euler dans tous ses efforts pour démontrer les théorèmes concernant le caractère de 2 (Voir Disq. Arithm., art. 120) est donc d'autant plus surprenant.

Un phénomène entièrement analogue se présente dans la théorie des résidus biquadratiques. Ici également, la loi générale de réci-

non divisibles par  $1+i$ , et le caractère de ce nombre premier particulier doit être déterminé séparément.

Dans le mémoire de Gauss: *Theoria residuorum biquadraticorum commentatio secunda*, où les nombres complexes entiers de la forme  $a+bi$  furent introduits pour la première fois dans la théorie des nombres, le caractère biquadratique de  $1+i$  est déterminé complètement. La démonstration y est de nature purement arithmétique et s'appuie essentiellement sur le théorème de l'art. 71, théorème analogue au lemme formant la base tant de la troisième que de la cinquième démonstration de Gauss pour la loi de réciprocité dans la théorie des résidus quadratiques (*Theorematis arithmetici demonstratio nova*. Werke, II, p. 1, et *Theorematis fundamentalis in doctrina de residuis quadraticis demonstrationes et ampliaciones novae* Werke, II, p. 47).

Comme on le sait, le troisième mémoire, dans lequel Gauss s'était proposé de donner la démonstration de la loi générale de réciprocité déjà énoncée dans son second mémoire sur cette théorie, n'a jamais paru.

Les deux premières démonstrations publiées de ce théorème fondamental sont celles d'Eisenstein, dans le tome 28 du *Journal für Mathematik* de Crelle, p. 53 et 223. Dans le premier article Lois de réciprocité, il n'a pas traité du caractère de  $1+i$ , mais bien dans le second article: *Einfacher Beweis und Verallgemeinerung des Fundamentaltheorems für die biquadratischen Reste*. Eisenstein fait usage, dans l'établissement du caractère de  $1+i$ , de la loi générale de réciprocité démontrée antérieurement, ce qui en tout cas paraît peu élégant, vu que le passage du simple au composé demande nécessairement que le caractère de  $1+i$  soit déduit d'une façon entièrement indépendante du théorème fondamental.

La même remarque est plus ou moins applicable à toutes les autres méthodes qui ont été employées postérieurement pour traiter la théorie des résidus biquadratiques; la marche suivie par Gauss pour démontrer le caractère de  $1+i$  est, à mon avis, la seule qui puisse être dite purement arithmétique et complètement indépendante d

loi générale de réciprocité, de sorte qu'une loi analogue, dans le rapport, aux conditions qui devront être imposées à tout développement méthodique de la théorie des résidus biquadratiques, prise dans son ensemble.

Des remarques tout à fait analogues peuvent être faites au sujet de la théorie des résidus cubiques. La première démonstration de la loi de réciprocité dans cette théorie — loi énoncée par Jacobi — est celle d'Eisenstein, publiée dans le tome 27 du Journal für Mathematik de Crelle, p. 289. La détermination particulière du caractère de  $1-\rho$ , où  $\rho$  est une racine cubique complexe de l'unité, n'a été donnée par Eisenstein que plus tard, dans le tome 28, p. 28 et suiv. du même journal. Pour cette détermination il fait encore usage de la loi générale de réciprocité, et je ne sache pas qu'on ait donné jusqu'ici un mode de déduction du caractère cubique de  $1-\rho$  dont la même chose ne puisse être dite.

Comme il est à désirer toutefois, qu'on possède une démonstration du caractère de  $1+i$  et de  $1-\rho$  entièrement indépendante de la loi générale de réciprocité, il y aura peut-être quelque intérêt à faire voir comment tous ces théorèmes relatifs aux nombres premiers 2,  $1+i$  et  $1-\rho$ , théorèmes nécessaires pour compléter les lois de réciprocité, peuvent être démontrés suivant une méthode uniforme.

Le principe de cette méthode consiste à remplacer le nombre premier, dont il s'agit de déterminer le caractère, par un produit congruent de facteurs. On détermine alors le caractère de ces facteurs par des considérations tout à fait analogues à celles dont Gauss s'est servi dans les art 15—20 de son premier mémoire sur la théorie des résidus biquadratiques (Werke, II, p. 78—87). Gauss n'y a en vue que les nombres réels, et l'objet de son mémoire est la détermination du caractère de 2 dans la théorie réelle. Mais j'ai reconnu que tous les raisonnements de Gauss se laissent reproduire aussi, presque sans changement, dans la théorie des nombres complexes, et la détermination du caractère biquadratique de  $1+i$  s'obtient alors immédiatement au moyen d'une considération très simple, suivant laquelle  $1+i$  est congru à un produit dont on connaît le caractère des facteurs.

les recherches du premier mémoire de Gauss, la détermination du caractère de  $1+i$  par rapport à un nombre premier de la forme  $a+bi$  (où  $b$  n'est pas égal à zéro) n'offre plus aucune difficulté. Une méthode entièrement analogue peut d'ailleurs être employée dans le cas où le module est un nombre premier réel de la forme  $4n+3$ . Bien que ce dernier cas permette une démonstration beaucoup plus simple (Voir, par ex., Gauss. Werke, II, art. 68), j'ai cru devoir le traiter de la même manière que les autres cas, pour faire ressortir que la méthode en question suffit à établir l'ensemble des théorèmes.

Après avoir effectué la détermination du caractère biquadratique de  $1+i$ , je démontre, à l'aide des développements antérieurs, tous les théorèmes que Gauss a trouvés par induction et énoncés dans l'art. 28 de la *Theoria residuorum biquadraticorum commentatio secunda*. Si je ne me trompe, cette démonstration est donnée ici pour la première fois<sup>1</sup>). Elle est entièrement fondée sur la théorie des nombres complexes, théorie qui joue donc ici un rôle purement auxiliaire, les théorèmes eux-mêmes ayant seulement rapport à des nombres réels. Outre la loi de réciprocité dans la théorie des résidus biquadratiques, la démonstration complète exigeait encore les considérations des art. 19—21.

Je vais maintenant commencer par déduire le caractère de 2 dans la théorie des

#### RÉSIDUS QUADRATIQUES.

1. Soit  $p$  un nombre premier impair, les nombres  
 $1, 2, 3, \dots, p-1$   
 seront alors divisés en deux groupes. Dans le premier groupe  
 A  $a, a', a'', \dots$   
 sont rapportés tous les résidus quadratiques, dans le second groupe  
 B  $\beta, \beta', \beta'', \dots$   
 tous les non-résidus, pour le module  $p$ . Chacun des groupes A et

<sup>1</sup>) Une partie de ces théorèmes a été démontrée par M. Lebesgue, dans le Journal de Liouville, t. 4, p. 51, 52, remarque 1°.

B se compose de  $\frac{p-1}{2}$  nombres incongrus par rapport au module  $p$ ,

et il est facile de voir que les deux congruences

$$(x - \alpha)(x - \alpha')(x - \alpha'') \dots \equiv x^{\frac{p-1}{2}} - 1 \pmod{p}$$

$$(x - \beta)(x - \beta')(x - \beta'') \dots \equiv x^{\frac{p-1}{2}} + 1 \pmod{p}$$

sont des congruences identiques; car elles sont de degré moins élevé que la  $\left(\frac{p-1}{2}\right)^{\text{ième}}$  et toutes les deux possèdent manifestement  $\frac{p-1}{2}$  racines, à savoir, la première les racines  $x = \alpha, x = \alpha', x = \alpha'', \dots$ , la seconde les racines  $x = \beta, x = \beta', x = \beta'', \dots$ .

En ajoutant l'unité aux nombres de A et de B, on obtient les groupes de nombres suivants

$$\begin{array}{ll} A' & \alpha + 1, \alpha' + 1, \alpha'' + 1, \dots \\ B' & \beta + 1, \beta' + 1, \beta'' + 1, \dots \end{array}$$

Le nombre des nombres du groupe A' qui font partie de A et de B sera désigné respectivement par (0.0), (0.1), et le nombre des nombres de B' qui entrent dans A et B respectivement par (1.0), (1.1).

Ces quatre nombres peuvent être réunis dans le tableau S suivant

$$\begin{array}{cc} (0.0) & (0.1) \\ (1.0) & (1.1). \end{array}$$

Comme les nombres premiers des formes  $p = 4n + 1$  et  $p = 4n + 3$  se comportent d'une manière différente, ces deux cas doivent être traités séparément. Commençons par le premier.

2. Pour  $p = 4n + 1$  le nombre  $-1$  est résidu quadratique, de sorte que les nombres  $\alpha$  et  $p - \alpha$  entrent simultanément dans A. De même, les nombres  $\beta$  et  $p - \beta$  entrent simultanément dans B.

Or (0.0) est évidemment égal au nombre de solutions de la congruence

$$\alpha + 1 \equiv \alpha' \pmod{p},$$

où  $\alpha$  et  $\alpha'$  doivent être choisis dans le groupe A; et comme on a  $\alpha' = p - \alpha''$ , on peut dire aussi que (0.0) représente le nombre de solutions de la congruence

$$\alpha + \alpha'' + 1 \equiv 0 \pmod{p}.$$

En raisonnant de la même manière par rapport aux nombres (0.1), (1.0), (1.1), on reconnaît que le

signe	représente le nombre des solutions de
(0.0)	$\alpha + \alpha' + 1 \equiv 0$
(0.1)	$\alpha + \beta + 1 \equiv 0$
(1.0)	$\beta + \alpha + 1 \equiv 0$
(1.1)	$\beta + \beta' + 1 \equiv 0$

(mod  $p$ ).

Il en ressort immédiatement

$$(0.1) = (1.0),$$

une seconde relation entre les nombres du schéma S est fournie par la considération suivante. A chaque nombre  $\beta$  du groupe B correspond, dans ce même groupe, un nombre déterminé unique  $\beta''$ , tel qu'on a

$$\beta \beta'' \equiv 1 \pmod{p},$$

et en outre,  $\beta' \beta''$  est alors congru à un nombre  $\alpha$  du groupe A. La multiplication de la congruence

$$\beta + \beta' + 1 \equiv 0$$

par  $\beta''$  donne donc

$$1 + \alpha + \beta'' \equiv 0,$$

et en multipliant cette dernière congruence par  $\beta$  on retrouve la première. De là se déduit immédiatement  $(1.1) = (0.1)$ , de sorte que le schéma S a la forme

$$\begin{array}{c} h j \\ j j. \end{array}$$

Or, dans le groupe A se trouve le nombre  $p-1$ , et par conséquent dans  $A'$  le nombre  $p$ , qui n'entre ni dans A ni dans B. Mais tous les autres nombres de  $A'$  et de  $B'$  font partie soit de A, soit de B.

Il en résulte

$$p-1$$

$$h = \frac{p-5}{4}, \quad j = \frac{p-1}{4}.$$

La congruence identique

$$(x - \beta)(x - \beta')(x - \beta'') \dots \equiv x^{\frac{p-1}{2}} + 1 \pmod{p}$$

donne maintenant pour  $x = -1$ , puisque  $\frac{p-1}{2}$  est pair,

$$(\beta + 1)(\beta' + 1)(\beta'' + 1) \dots \equiv 2 \pmod{p}.$$

Le nombre des non-résidus parmi les nombres  $\beta + 1, \beta' + 1, \beta'' + 1, \dots$  est (1.1)  $= j = \frac{p-1}{4}$ .

Si donc  $j$  est pair, ou

$$p = 8n + 1,$$

2 est résidu quadratique de  $p$ .

Si, au contraire  $j$  est impair, ou

$$p = 8n + 5,$$

2 est non-résidu de  $p$ .

3. Pour  $p = 4n + 3$  le nombre  $-1$  est non-résidu, et le groupe E est identique au groupe des nombres  $p - a, p - a', p - a'', \dots$

Le signe (0.0) représente alors le nombre des solutions de la congruence  $a + 1 \equiv a' \pmod{p}$  ou aussi, puisque  $a' = p - \beta$ , le nombre des solutions de  $a + \beta + 1 \equiv 0$ .

On voit ainsi que le

signe	représente le nombre des solutions de
(0.0)	$a + \beta + 1 \equiv 0$
(0.1)	$a + a' + 1 \equiv 0 \pmod{p},$
(1.0)	$\beta + \beta' + 1 \equiv 0$
(1.1)	$\beta + a + 1 \equiv 0$

de sorte que (0.0) = (1.1). Si, en outre, on a de nouveau  $\beta\beta'' \equiv 1$ ,  $\beta'\beta'' \equiv a$ , la congruence  $\beta + \beta' + 1 \equiv 0$ , étant multipliée par  $\beta''$ , donne

$$1 + a + \beta'' = 0$$

Il résulte, d'une manière analogue à celle indiquée dans le cas précédent, la relation  $(1.0) = (0.0)$ . Le schéma S a donc pour  $p = 4n + 1$  la forme

$$\begin{array}{c} h \ j \\ h \ h. \end{array}$$

Comme le nombre  $p - 1$  entre dans le groupe B, et par conséquent dans B', mais que d'ailleurs tous les autres nombres de A' et de B' entrent soit dans A, soit dans B, on trouve

$$h + j = \frac{p-1}{2},$$

$$2h = \frac{p-1}{2} - 1,$$

donc

$$h = \frac{p-3}{4}, \quad j = \frac{p+1}{4}.$$

Dans la congruence identique

$$(x - \alpha)(x - \alpha')(x - \alpha'') \dots \equiv x^{\frac{p-1}{2}} - 1 \pmod{p}$$

il résulte pour  $x = -1$ , vu que  $\frac{p-1}{2}$  est impair,

$$(\alpha + 1)(\alpha' + 1)(\alpha'' + 1) \dots \equiv 2 \pmod{p},$$

et le nombre des non-résidus, parmi les nombres  $\alpha + 1, \alpha' + 1, \alpha'' + 1, \dots$

est  $(0.1) = j = \frac{p+1}{4}$ .

Si l'on a donc  $j$  pair, ou

$$p = 8n + 7,$$

2 est résidu quadratique de  $p$ .

Si, au contraire,  $j$  est impair, ou

$$p = 8n + 3,$$



4. Le nombre premier impair (c'est-à-dire non divisible par  $1 + i$ )  $m = a + bi$  sera toujours supposé primaire; ce mot étant pris dans l'acception qui lui est donnée par Gauss, de sorte que  $a - 1$  et  $b$  suivant le module 4, soient ou bien tous les deux  $\equiv 0$ , ou bien tous les deux  $\equiv 2$ .

On sait que, dans la théorie des nombres complexes entiers de la forme  $a + bi$ , les nombres premiers se composent :

premièrement, des nombres premiers réels  $q$  de la forme  $4r + 3$  nombres qui doivent être pris négativement pour être primaires;

secondement, des facteurs premiers complexes des nombres premiers réels de la forme  $4n + 1$ . Ces nombres premiers complexes sont de la forme  $a + bi$ , où  $b$  n'est pas égal à zéro, et deviennent primaires lorsqu'on les multiplie par l'une des quatre unités  $1, i, -1, -i$ , convenablement choisie. Ils peuvent à leur tour être distingués en deux espèces, suivant que, lorsque  $a + bi$  est primaire  $a - 1$  et  $b$  sont tous les deux divisibles par 4, ou tous les deux le double d'un nombre impair.

D'après cela, je partage les nombres premiers primaires en ces trois classes :

- I. Les nombres premiers réels  $q$  de la forme  $4r + 3$ , pris négativement.
- II. Les nombres premiers complexes de la forme  $4r + 1 + 4si$
- III. Les nombres premiers complexes de la forme  $4r + 3 + (4s + 2)i$ .

Le nombre premier (dans la théorie complexe) sera toujours désigné ici par  $M$ , la norme de  $M$  par  $\mu$ . En outre,  $p$  représentera toujours un nombre premier réel (positif) de la forme  $4r + 1$ ,  $q$  un nombre premier réel (positif) de la forme  $4r + 3$ . Pour les nombres premiers de la première espèce, on a donc  $M = -q$ ,  $\mu = q^2$ , pour ceux de la deuxième et de la troisième espèce  $\mu = p$ .

Je remarquerai encore que pour les deux espèces I et II la norme  $\mu$  est de la forme  $8r + 1$ , et pour III de la forme  $8r + 5$ . Cette circonstance fait que les deux premières espèces de nombres premiers peuvent, jusqu'à un certain point, être traitées conjointement.

être égal, aux trois classes de nombres premiers.

5. Soient donc  $M$  le nombre premier,  $\mu$  la norme. Un système complet de nombres incongrus et non divisibles par le module  $M$  se compose de  $\mu - 1$  nombres qui, suivant leur caractère biquadratique par rapport à  $M$ , peuvent être distribués en quatre classes, comprenant chacune  $\frac{\mu - 1}{4}$  nombres

A	$\alpha, \alpha', \alpha'', \dots$
B	$\beta, \beta', \beta'', \dots$
C	$\gamma, \gamma', \gamma'', \dots$
D	$\delta, \delta', \delta'', \dots$

Dans la première classe A sont rangés tous les nombres  $\alpha, \alpha', \alpha'', \dots$  de caractère biquadratique 0, dans les groupes B, C, D les nombres de caractère biquadratique 1, 2, 3.

Disons encore, par surcroît, que le caractère biquadratique est pris ici dans le sens adopté par Gauss, de sorte que les nombres des quatre classes sont caractérisés par les congruences

$$\alpha^{\frac{\mu-1}{4}} \equiv 1, \beta^{\frac{\mu-1}{4}} \equiv i, \gamma^{\frac{\mu-1}{4}} \equiv -1, \delta^{\frac{\mu-1}{4}} \equiv -i \pmod{M}.$$

Pour plus de commodité, je me servirai toutefois aussi du symbole introduit par Jacobi, et pourrai donc écrire

$$\left(\left(\frac{\alpha}{M}\right)\right) = 1, \left(\left(\frac{\beta}{M}\right)\right) = i, \left(\left(\frac{\gamma}{M}\right)\right) = -1, \left(\left(\frac{\delta}{M}\right)\right) = -i.$$

Notons enfin, une fois pour toutes, que dans la suite toutes les congruences auront rapport au module premier  $M$ , tant qu'un autre module ne sera pas expressément indiqué.

Je donne ici un exemple de la distribution des résidus  $(\text{mod } M)$ , à l'exception du résidu 0, dans les quatre classes A, B, C, D, pour chacune des trois espèces de nombre premiers qui ont été distinguées dans le n° 4.

$$\begin{array}{ccccccc} & & M = -7, & & \mu = 49. & & \\ A & 1, & -2, & -3, & -1, & 2, & 3, \\ & 3i, & i, & -2i, & -3i, & -i, & 2i \end{array}$$

	$-1+3i,$	$2+i,$	$3-2i,$	$1-3i,$	$-2-i,$	$-3+2i,$
C	$-3+3i,$	$-1+i,$	$2-2i,$	$3-3i,$	$1-i,$	$-2+2i,$
	$-2-2i,$	$-3-3i,$	$-1-i,$	$2+2i,$	$3+3i,$	$1+i,$
D	$3+2i,$	$1+3i,$	$-2+i,$	$-3-2i,$	$-1-3i,$	$2-i,$
	$1+2i,$	$-2+3i,$	$-3+i,$	$-1+2i,$	$2-3i,$	$3-i,$

$$M = -3 - 8i, \quad \mu = 73.$$

	$1,$	$-3i,$	$-1-3i,$	$-1,$	$3i,$	$1+3i,$
A	$3+2i,$	$1+2i,$	$-2,$	$-3-2i,$	$-1-2i,$	$2,$
	$-1-4i,$	$-4,$	$-3+4i,$	$1+4i,$	$4,$	$3-4i,$
	$1-2i,$	$5+2i,$	$1-4i,$	$-1+2i,$	$-5-2i,$	$-1+4i,$
B	$-1-i,$	$-3+3i,$	$-2+4i,$	$1+i,$	$3-3i,$	$2-4i,$
	$2+3i,$	$1-3i,$	$2+2i,$	$-2-3i,$	$-1+3i,$	$-2-2i,$
	$4i,$	$4+3i,$	$4-i,$	$-4i,$	$-4-3i,$	$-4+i,$
C	$-3+i,$	$i,$	$3,$	$3-i,$	$-i,$	$-3,$
	$2i,$	$-2+3i,$	$-2+i,$	$-2i,$	$2-3i,$	$2-i,$
	$-3-i,$	$2-2i,$	$-3+2i,$	$3+i,$	$-2+2i,$	$3-2i,$
D	$-4-i,$	$2+i,$	$-2+5i,$	$4+i,$	$-2-i,$	$2-5i,$
	$4+2i,$	$1-i,$	$-3-3i,$	$-4-2i,$	$-1+i,$	$3+3i,$

$$M = -5 + 6i, \quad \mu = 61.$$

	$1,$	$-3,$	$-2+i,$	$1+3i,$	$-2+2i,$
A	$-4,$	$1+i,$	$3+2i,$	$-3-i,$	$3-2i,$
	$-1-4i,$	$2+i,$	$2i,$	$-5,$	$4+i,$
	$1-i,$	$2-3i,$	$-1+3i,$	$-2-3i,$	$4i,$
B	$1-2i,$	$2,$	$5i,$	$1-4i,$	$-4+i,$
	$1+2i,$	$3-i,$	$2+2i,$	$-i,$	$3i,$
	$-2i,$	$5,$	$-4-i,$	$1+4i,$	$-2-i,$
	$-1-3i,$	$2-2i,$	$-1,$	$3,$	$2-i,$
	$3+i,$	$-3+2i,$	$4,$	$-1-i,$	$-3-2i,$
	$-2-2i,$	$i,$	$-3i,$	$-1-2i,$	$-3+i,$
	$2+3i,$	$-4i,$	$-1+i,$	$-2+3i,$	$1-3i,$
	$-1+4i,$	$4-i,$	$-1+2i,$	$-2,$	$-5i,$

De même qu'au n° 1, on se convainc immédiatement de l'identité des congruences suivantes

$$\begin{aligned}
 (x - \alpha)(x - \alpha')(x - \alpha'') \dots &\equiv x^{\frac{\mu-1}{4}} - 1 \\
 (x - \beta)(x - \beta')(x - \beta'') \dots &\equiv x^{\frac{\mu-1}{4}} - i \\
 (x - \gamma)(x - \gamma')(x - \gamma'') \dots &\equiv x^{\frac{\mu-1}{4}} + 1 \\
 (x - \delta)(x - \delta')(x - \delta'') \dots &\equiv x^{\frac{\mu-1}{4}} + i
 \end{aligned} \pmod{M},$$

d'où il suit pour  $x = -1$ , en distinguant les cas  $\mu = 8n + 1$  et  $\mu = 8n + 5$

$$\begin{aligned}
 \mu = 8n + 1 \quad & (\beta + 1)(\beta' + 1)(\beta'' + 1) \dots \equiv 1 - i \\
 & (\gamma + 1)(\gamma' + 1)(\gamma'' + 1) \dots \equiv 2 \\
 & (\delta + 1)(\delta' + 1)(\delta'' + 1) \dots \equiv 1 + i \\
 \mu = 8n + 5 \quad & (\alpha + 1)(\alpha' + 1)(\alpha'' + 1) \dots \equiv 2 \\
 & (\beta + 1)(\beta' + 1)(\beta'' + 1) \dots \equiv 1 + i \\
 & (\delta + 1)(\delta' + 1)(\delta'' + 1) \dots \equiv 1 - i
 \end{aligned} \pmod{M}.$$

6. Considérons maintenant les nouveaux groupes de nombres  $A', B', C'$  et  $D'$  qui résultent de l'addition de l'unité aux nombres de  $A, B, C$  et  $D$

$$\begin{aligned}
 A' & \alpha + 1, \alpha' + 1, \alpha'' + 1, \dots \\
 B' & \beta + 1, \beta' + 1, \beta'' + 1, \dots \\
 C' & \gamma + 1, \gamma' + 1, \gamma'' + 1, \dots \\
 D' & \delta + 1, \delta' + 1, \delta'' + 1, \dots
 \end{aligned}$$

Désignons le nombre des nombres de  $A'$  qui sont congrus à des nombres de  $A, B, C, D$  respectivement par

$$(0.0), (0.1), (0.2), (0.3);$$

et le nombre des nombres de  $B'$  qui sont congrus à des nombres de  $A, B, C, D$  respectivement par

$$(1.0), (1.1), (1.2), (1.3).$$

De même, les nombres

$$(2.0), (2.1), (2.2), (2.3)$$

auront rapport au groupe  $C'$ , et

$$(3.0), (3.1), (3.2), (3.3)$$

Ces 16 nombres (0.0), (0.1), etc. peuvent être tous réunis dans un tableau quadratique S suivant

(0.0)	(0.1)	(0.2)	(0.3)
(1.0)	(1.1)	(1.2)	(1.3)
(2.0)	(2.1)	(2.2)	(2.3)
(3.0)	(3.1)	(3.2)	(3.3)

et pour les exemples donnés au n<sup>o</sup> 5, j'obtiens

	$M = -7, \mu = 49.$				$M = -3 - 8i, \mu = 73.$				$M = -5 + 6i, \mu = 61.$			
S	5	2	2	2	5	6	4	2	4	3	2	6
	2	2	4	4	6	2	5	5	3	3	6	3
	2	4	2	4	4	5	4	5	4	3	4	3
	2	4	4	2	2	5	5	6	3	6	3	3

D'après les congruences du numéro précédent, on a  
pour  $\mu = 8n + 1$

$$(\delta + 1)(\delta' + 1)(\delta'' + 1) \dots \equiv 1 + i$$

et pour  $\mu = 8n + 5$

$$(\beta + 1)(\beta' + 1)(\beta'' + 1) \dots \equiv 1 + i.$$

Or, le nombre des nombres de

$$\delta + 1, \delta' + 1, \delta'' + 1, \dots$$

qui appartiennent respectivement aux classes A, B, C, D, étant (3.0), (3.1), (3.2), (3.3), il s'ensuit immédiatement que pour  $\mu = 8n + 1$  le caractère biquadratique de  $1 + i$ , suivant le module 4, sera congru à

$$(3.1) + 2(3.2) + 3(3.3)$$

et de même, dans le cas de  $\mu = 8n + 5$ , congru à

$$(1.1) + 2(1.2) + 3(1.3).$$

Dès que les nombres (0.0), (0.1), ... seront déterminés, le caractère biquadratique de  $1 + i$  sera donc aussi immédiatement connu.

Il s'agit donc, étant donné le nombre premier primaire  $M = a + bi$ , d'en déduire directement les nombres du tableau S. Les considérations nécessaires à cet effet sont essentiellement les mêmes que celles développées par Gauss dans les art. 16—20 de la *Theoria residuorum biquadraticorum commentatio prima*.

mais il est facile de voir que ce qu'il y donne est dans un étroit rapport avec la question dont nous nous occupons en ce moment.

Pour avoir sous les yeux le développement complet, il sera nécessaire de reproduire ici l'argumentation de Gauss, avec les légères modifications réclamées par la différence des sujets.

Il faut remarquer, à cet égard, que pour un nombre premier  $M = -q$  appartenant à la première classe du n° 4, il n'existe, dans la théorie réelle de Gauss, rien d'analogue à ce qui sera exposé ici dans la théorie des nombres complexes entiers.

Pour ce qui va suivre, il est nécessaire de traiter séparément les cas où la norme  $\mu$  est de la forme  $8n + 1$  et celui où elle est de la forme  $8n + 5$ . Je commence par le premier dans lequel le nombre premier  $M$  appartient donc à l'une des deux premières classes du n° 4.

7. Pour  $\mu = 8n + 1$ , on a  $(-1)^{\frac{\mu-1}{4}} = +1$ , de sorte que  $-1$  est un résidu biquadratique de  $M$  et fait partie de la classe A, ou à proprement parler, est congru suivant le module  $M$  à un nombre de la classe A. Mais, dans ce genre de considérations, il est permis, attendu que les nombres congrus entre eux peuvent se remplacer, de le regarder comme égaux, et pour la commodité je ferai usage de cette observation, dont il ne pourra résulter aucune obscurité.

Le caractère biquadratique de  $-1$  étant donc égal à zéro, il s'ensuit que lorsque  $\alpha, \beta, \gamma, \delta$  appartiennent respectivement aux classes A, B, C, D, les nombres  $-\alpha, -\beta, -\gamma, -\delta$  entrent aussi dans ces mêmes classes,  $-\alpha$  dans A,  $-\beta$  dans B,  $-\gamma$  dans C et  $-\delta$  dans D. Or, le nombre (0.0) est évidemment égal au nombre des solutions de la congruence

$$\alpha + 1 \equiv \alpha' \pmod{M},$$

où  $\alpha$  et  $\alpha'$  sont à prendre arbitrairement dans le groupe A; mais comme à chaque nombre  $\alpha'$  correspond un nombre  $\alpha'' = p - \alpha'$ , le nombre de solutions est le même que celui de la congruence

$$\alpha + \alpha'' + 1 \equiv 0 \pmod{M},$$

où  $\alpha$  et  $\alpha''$  doivent également être pris dans A.

En raisonnant exactement de la même manière au sujet des nombres (0.1), (0.2), etc., on trouve que le

signe	représente le nombre des solutions de	
(0.0)	$\alpha + \alpha' + 1 \equiv 0$	
(0.1)	$\alpha + \beta + 1 \equiv 0$	
(0.2)	$\alpha + \gamma + 1 \equiv 0$	
(0.3)	$\alpha + \delta + 1 \equiv 0$	
(1.0)	$\beta + \alpha + 1 \equiv 0$	
(1.1)	$\beta + \beta' + 1 \equiv 0$	
(1.2)	$\beta + \gamma + 1 \equiv 0$	
(1.3)	$\beta + \delta + 1 \equiv 0$	
(2.0)	$\gamma + \alpha + 1 \equiv 0$	(mod M).
(2.1)	$\gamma + \beta + 1 \equiv 0$	
(2.2)	$\gamma + \gamma' + 1 \equiv 0$	
(2.3)	$\gamma + \delta + 1 \equiv 0$	
(3.0)	$\delta + \alpha + 1 \equiv 0$	
(3.1)	$\delta + \beta + 1 \equiv 0$	
(3.2)	$\delta + \gamma + 1 \equiv 0$	
(3.3)	$\delta + \delta' + 1 \equiv 0$	

Il en résulte donc immédiatement ces six relations

$$\begin{aligned} (0.1) &= (1.0), & (0.2) &= (2.0), & (0.3) &= (3.0), \\ (1.2) &= (2.1), & (1.3) &= (3.1), \\ (2.3) &= (3.2). \end{aligned}$$

Cinq autres relations entre les nombres (0.0), (0.1), etc. s'obtiennent par la considération suivante. Si  $\alpha, \beta, \gamma$  sont des nombres de A, B, C, et qu'on détermine  $x, y, z$  de telle sorte qu'on ait

$$\alpha x \equiv 1, \beta y \equiv 1, \gamma z \equiv 1 \pmod{M},$$

$x$  appartient évidemment à la classe A,  $y$  à D,  $z$  à C, de sorte qu'on peut écrire

$$\alpha \alpha' \equiv 1, \beta \delta \equiv 1, \gamma \gamma' \equiv 1.$$

Si l'on multiplie maintenant, en considérant une solution déterminée de  $\alpha + \beta + 1 \equiv 0$ , cette congruence par  $\delta$ , on obtient  $\delta' + 1 + \delta \equiv 0$  où  $\delta' \equiv \alpha \delta$  appartient à D. Réciproquement  $\delta' + 1 + \delta \equiv 0$ , multiplié par  $\beta$ , donne de nouveau  $\alpha + \beta + 1 \equiv 0$ . Il ressort de là que les deux congruences

$$\alpha + \beta + 1 \equiv 0 \text{ et } \delta + \delta' + 1 \equiv 0$$

ont le même nombre de solutions, ou (0.1) = (2.2).

Exactement de la même manière, on a

$$\begin{aligned}\gamma' (a + \gamma + 1) &\equiv \gamma'' + 1 + \gamma', \\ \beta (a + \delta + 1) &\equiv \beta' + 1 + \beta, \\ \delta (\beta + \gamma + 1) &\equiv 1 + \beta' + \delta, \\ \gamma' (\beta + \gamma + 1) &\equiv \delta + 1 + \gamma',\end{aligned}$$

d'où l'on conclut pareillement

$$(0.2) = (2.2), \quad (0.3) = (1.1), \quad (1.2) = (1.3) = (2.3).$$

En tout, il existe donc onze relations entre les seize nombres du schéma S, et ces nombres sont ainsi ramenés à cinq, différents entre eux, qui seront désignés par  $h, j, k, l, m$ . Le schéma S prend alors cette forme

$h$	$j$	$k$	$l$
$j$	$l$	$m$	$m$
$k$	$m$	$k$	$m$
$l$	$m$	$m$	$j$

8. Le nombre  $-1$  entre dans A, et correspond donc au nombre 0 de A'. Ce nombre 0 de A' ne se trouve dans aucune des classes A, B, C, D, mais tout autre nombre de A' entre évidemment dans l'un des groupes A, B, C ou D. Comme  $\mu = 8n + 1$ ,  $\frac{\mu - 1}{4} = 2n$ , on a donc

$$(0.0) + (0.1) + (0.2) + (0.3) = 2n - 1.$$

Tous les nombres de B', C', D' font partie d'une des classes A, B, C, D, de sorte qu'on a

$$\begin{aligned}(1.0) + (1.1) + (1.2) + (1.3) &= 2n, \\ (2.0) + (2.1) + (2.2) + (2.3) &= 2n, \\ (3.0) + (3.1) + (3.2) + (3.3) &= 2n.\end{aligned}$$

Ces quatre équations se réduisent aux trois relations suivantes entre  $h, j, k, l$  et  $m$



congruence

$$\alpha + \beta + \gamma + 1 \equiv 0 \pmod{M},$$

où  $\alpha, \beta, \gamma$  doivent être choisis de toutes les manières possibles dans les classes A, B, C.

Si l'on prend d'abord pour  $\alpha$  successivement tous les nombres de la classe A, il arrive respectivement  $h, j, k, l$  fois que  $\alpha + 1$  appartient à A, B, C, D, et le cas unique de  $\alpha + 1 \equiv 0$  peut être négligé, vu que la congruence  $\beta + \gamma \equiv 0$  n'admet aucune solution.

Pour chacune des  $h$  valeurs qui rendent  $\alpha + 1 \equiv \alpha_0$ ,  $\beta$  et  $\gamma$  doivent alors être choisis de façon qu'on ait

$$\alpha_0 + \beta + \gamma \equiv 0.$$

Le nombre des solutions de cette congruence (pour une valeur donnée de  $\alpha_0$ ) est égal à  $m$ , comme on le reconnaît immédiatement en la multipliant par  $\alpha'_0$ , ce qui la transforme, à cause de  $\alpha_0 \alpha'_0 \equiv 1 \pmod{M}$ , en

$$1 + \beta' + \gamma' \equiv 0.$$

Comme ce raisonnement est applicable à chacune des  $h$  valeurs qui font que  $\alpha + 1$  appartient de nouveau à A, on obtient de cette manière  $hm$  solutions de la congruence

$$1 + \alpha + \beta + \gamma \equiv 0.$$

Il arrive ensuite  $j$  fois que  $\alpha + 1$  appartienne à B, et pour chaque valeur déterminée  $\alpha + 1 \equiv \beta_0$  la congruence

$$\beta_0 + \beta + \gamma \equiv 0$$

a le même nombre de solutions que celle-ci

$$1 + \alpha + \beta' \equiv 0,$$

ce nombre est donc égal à  $j$ . Cela ressort immédiatement de

$$\delta_0(\beta_0 + \beta + \gamma) \equiv 1 + \alpha + \beta',$$

lorsque  $\beta_0 \delta_0 \equiv 1$ .

Ces valeurs de  $\alpha$ , qui font appartenir  $\alpha + 1$  à B, donnent donc en tout  $jj$  solutions de la congruence considérée.

Pour  $\alpha + 1 \equiv \gamma_0$ , ce qui arrive  $k$  fois, la congruence

$$\gamma_0 + \beta + \gamma \equiv 0$$

$$\gamma'_0(\gamma_0 + \beta + \gamma) \equiv 1 + \delta + \alpha.$$

Les valeurs de  $\alpha$  qui font appartenir  $\alpha + 1$  à C fournissent donc en tout  $kl$  solutions.

A-t-on enfin  $\alpha + 1 = \delta_0$ , ce qui arrive  $l$  fois, alors la congruence

$$\delta_0 + \beta + \gamma \equiv 0$$

a, en raison de

$$\beta_0(\delta_0 + \beta + \gamma) \equiv 1 + \gamma + \delta,$$

$m$  solutions, et ces valeurs de  $\alpha$  donnent donc  $lm$  solutions.

Le nombre total des solutions de la congruence

$$\alpha + \beta + \gamma + 1 \equiv 0 \pmod{M}$$

est donc

$$hm + jj + kl + lm.$$

Mais ce nombre peut encore être calculé d'une autre manière. Si l'on prend pour  $\beta$  successivement tous les nombres de B, il arrive,  $l$ ,  $m$ ,  $m$  fois que  $\beta + 1$  appartienne aux groupes A, B, C, D. Or pour chacun de ces quatre nombres, on trouve qu'il y a respectivement  $k$ ,  $m$ ,  $k$ ,  $m$  solutions de la congruence donnée, de sorte que le nombre total des solutions est

$$jk + lm + mk + mm.$$

10. En égalant entre elles ces deux expressions du nombre de solutions de  $\alpha + \beta + \gamma + 1 \equiv 0$ , on a

$$0 = hm + jj + kl - jk - km - mm,$$

ou, si l'on élimine  $h$  à l'aide de la valeur  $h = 2m - k - 1$ , qu'on se déduit facilement des équations obtenues dans le n° 8 entre  $h$ ,  $j$ ,  $k$ ,  $l$ ,  $m$ ,

$$0 = (k - m)^2 + jj + kl - jk - kk - m.$$

D'après les relations du n° 8, on a

$$k = \frac{1}{2}(j + l)$$

et cette valeur étant substituée dans  $jj + kl - jk - kk$ , cette expression devient égale à  $\frac{1}{4}(l - j)^2$ , de sorte que l'équation précédente, après multiplication par 4, se transforme en

$$0 = 4(k - m)^2 + (l - j)^2 - 4m;$$

mais on a

$$4m = 2(k+m) - 2(k-m) = 2n - 2(k-m),$$

par conséquent

$$2n = 4(k-m)^2 + 2(k-m) + (l-j)^2,$$

ou bien

$$\mu = 8n + 1 = [4(k-m) + 1]^2 + 4(l-j)^2,$$

et, en posant

$$4(k-m) + 1 = A, \quad 2(l-j) = B,$$

il vient donc

$$\mu = A^2 + B^2.$$

Dans cette équation on a  $A \equiv 1 \pmod{4}$ , et B pair.

Il est maintenant facile d'exprimer  $h, j, k, l, m$  en A et B, ce qu'on donne

$$8h = 4n - 3A - 5,$$

$$8j = 4n + A - 2B - 1,$$

$$8k = 4n + A - 1,$$

$$8l = 4n + A + 2B - 1,$$

$$8m = 4n - A + 1.$$

Jusqu'ici nous avons seulement supposé que la norme  $\mu$  avait la forme  $8n + 1$ ; mais, pour la détermination ultérieure de A et B, il faut maintenant traiter séparément les cas I et II du n° 4.

11. Soit donc, en premier lieu

$$M = -q = -(4r + 3).$$

Dans ce cas, on a

$$\mu = M^2 = q^2$$

et par conséquent

$$q^2 = A^2 + B^2.$$

Le nombre  $q$  étant un nombre premier de la forme  $4r + 3$ , on sait que  $q^2$  ne peut être représenté que d'une seule manière comme la somme de deux carrés, savoir, en prenant  $\pm q$  pour la base du carré impair, et pour la base de l'autre carré 0; effectivement, si aucun des deux nombres A et B n'était égal à zéro ou divisible par  $q$ , on pourrait déterminer un nombre  $x$ , différent de zéro, de telle sorte que

$$Ax \equiv B \pmod{q}.$$

Mais de  $q^2 = A^2 + B^2$ , il suit

$$A^2 \equiv -B^2 \pmod{q}$$

$$A^2 x^2 \equiv B^2 \pmod{q},$$

par conséquent on aurait

$$x^2 \equiv -1 \pmod{q}.$$

Or, cette dernière congruence est impossible, parce que  $-1$  est un non-résidu quadratique de  $q$ .

De  $q^2 = A^2 + B^2$  il suit donc nécessairement

$$A = \pm q, \quad B = 0,$$

et comme  $A \equiv 1 \pmod{4}$ , le signe de  $A$  se trouve complètement déterminé et on a

$$A = -q = M.$$

$A$  et  $B$  étant ainsi trouvés, on a finalement

$$8h = 4n - 3M - 5,$$

$$8j = 4n + M - 1,$$

$$8k = 4n + M - 1,$$

$$8l = 4n + M - 1,$$

$$8m = 4n - M + 1,$$

où  $8n + 1 = M^2$ .

Par ces formules, la dépendance entre les nombres du tableau S et le nombre premier  $M$  est donc exprimée de la manière la plus simple, dans le cas où  $M$  appartient à la première classe du  $n^0$  4.

12. Si, en second lieu, on suppose  $M = a + bi$ , où  $a - 1 \equiv b \equiv 0 \pmod{4}$  et où la norme  $\mu = a^2 + b^2$  est un nombre premier réel, on a donc

$$\mu = a^2 + b^2 = A^2 + B^2.$$

Or, un nombre premier de la forme  $4k + 1$  ne peut être représenté que d'une seule manière par la somme de deux carrés, et comme  $a$  et  $A$  sont tous les deux  $\equiv 1 \pmod{4}$ , il s'ensuit  $A = a, B = \pm b$ .

Le signe de  $B$  est déterminé par les considérations suivantes, qui demandent la démonstration préalable de cette proposition auxiliaire

Lorsque  $z$  parcourt un système complet de résidus  $\pmod{M}$ , à l'exception du terme divisible par  $M$ , on a

$$\sum z^t \equiv -1 \quad \text{ou} \quad \equiv 0 \pmod{M},$$

suivant que  $t$  est divisible ou non par  $\mu - 1$ .

divisible par  $\mu - 1$ , on a  $z^t \equiv 1$ , donc  $\Sigma z^t \equiv \mu - 1 \equiv -1 \pmod{M}$ .

Pour démontrer aussi la seconde partie, soit  $g$  une racine primitive pour le nombre premier  $M$ , de sorte que les valeurs parcourues par  $z$  soient congrues à

$$g^0, g^1, g^2, g^3, \dots, g^{\mu-2}.$$

Il en résulte

$$\Sigma z^t \equiv 1 + g^t + g^{2t} + \dots + g^{(\mu-2)t} \pmod{M},$$

ou

$$(1 - g^t) \Sigma z^t \equiv 1 - g^{(\mu-1)t} \equiv 0 \pmod{M}.$$

Or, si  $t$  n'est pas divisible par  $\mu - 1$ ,  $1 - g^t$  n'est pas divisible par  $M$ , et on a par conséquent  $\Sigma z^t \equiv 0$  c. q. f. d.

Cette proposition auxiliaire est évidemment valable pour un nombre premier  $M$  quelconque.

D'après le développement binomial, on a maintenant

$$(z^2 + 1)^{\frac{\mu-1}{4}} = z^{\frac{\mu-1}{2}} + \dots + 1,$$

d'où il suit, lorsque le signe  $\Sigma$  se rapporte aux mêmes valeurs de  $z$  que tout à l'heure,

$$\Sigma (z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1 \pmod{M}.$$

Mais, d'un autre côté, les nombres  $z^2$ , dans leur ensemble, forment évidemment tous les nombres des groupes A et C, chacun de ces nombres étant pris deux fois. Des nombres

$$z^2 + 1$$

il y en a donc

$2(0.0) + 2(2.0)$  qui appartiennent à A,

$2(0.1) + 2(2.1)$  " " B,

$2(0.2) + 2(2.2)$  " " C,

$2(0.3) + 2(2.3)$  " " D,

et comme les puissances  $\frac{\mu-1}{4}$  des nombres de A, B, C, D sont respectivement congrues à 1,  $i$ ,  $-1$ ,  $-i$ , on a donc

$$\begin{aligned} \Sigma (z^2 + 1)^{\frac{\mu-1}{4}} &\equiv 2 [(0.0) + (2.0) - (0.2) - (2.2)] + \\ &\quad + 2i [(0.1) + (2.1) - (0.3) - (2.3)] \\ &\equiv 2 (h - k) + 2i (j - l). \end{aligned}$$

$$\Sigma(z^2 + 1)^{\frac{\mu-1}{4}} \equiv -a - 1 - Bi.$$

De la comparaison avec le premier résultat,

$$\Sigma(z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1,$$

il suit

$$a + Bi \equiv 0 \pmod{M = a + bi},$$

donc

$$B = b.$$

Par là, les valeurs de  $h, j, k, l, m$  du  $n^0 10$  se transforment finalement en

$$8h = 4n - 3a - 5,$$

$$8j = 4n + a - 2b - 1,$$

$$8k = 4n + a - 1,$$

$$8l = 4n + a + 2b - 1,$$

$$8m = 4n - a + 1,$$

où  $8n + 1 = a^2 + b^2$  est donc la norme du nombre premier  $M$ .

13. Après avoir traité les deux cas dans lesquels  $\mu = 8n + 1$  faut maintenant considérer le cas  $\mu = 8n + 5$ .

Puisque  $\frac{\mu-1}{4}$  est alors impair,  $-1$  appartient au groupe  $C$ , comme il est facile de le voir, les nombres

$$p - \alpha, p - \alpha', p - \alpha'', \dots$$

appartiennent tous à  $C$ , tandis que

$$p - \beta, p - \beta', p - \beta'', \dots$$

appartiennent tous à  $D$ .

Moyennant ces remarques, on reconnaît sans peine que le

signe	représente le nombre des solutions de	
(0.0)	$a + \gamma + 1 \equiv 0$	
(0.1)	$a + \delta + 1 \equiv 0$	
(0.2)	$a + \alpha' + 1 \equiv 0$	
(0.3)	$a + \beta + 1 \equiv 0$	
(1.0)	$\beta + \gamma + 1 \equiv 0$	(mod $M$ ),
(1.1)	$\beta + \delta + 1 \equiv 0$	
(1.2)	$\beta + \alpha + 1 \equiv 0$	
(1.3)	$\beta + \beta' + 1 \equiv 0$	

$$\begin{aligned}
(2.1) \quad & \gamma + \delta + 1 \equiv 0 \\
(2.2) \quad & \gamma + \alpha + 1 \equiv 0 \\
(2.3) \quad & \gamma + \beta + 1 \equiv 0 \\
(3.0) \quad & \delta + \gamma + 1 \equiv 0 \\
(3.1) \quad & \delta + \delta' + 1 \equiv 0 \\
(3.2) \quad & \delta + \alpha + 1 \equiv 0 \\
(3.3) \quad & \delta + \beta + 1 \equiv 0,
\end{aligned} \quad (\text{mod } M),$$

coulent les six relations

$$\begin{aligned}
(0.0) &= (2.2), & (0.1) &= (3.2), & (0.3) &= (1.2), \\
(1.0) &= (2.3), & (1.1) &= (3.3), \\
(2.1) &= (3.0).
\end{aligned}$$

e, de même que précédemment,  $\alpha \alpha' \equiv \beta \delta \equiv \gamma \gamma' \equiv 1$ , on a

$$\begin{aligned}
\gamma' (\alpha + \gamma + 1) &\equiv \gamma'' + 1 + \gamma', \\
\beta (\alpha + \delta + 1) &\equiv \beta' + 1 + \beta, \\
\delta (\alpha + \beta + 1) &\equiv \delta' + 1 + \delta, \\
\delta (\beta + \gamma + 1) &\equiv 1 + \beta' + \delta, \\
\gamma' (\beta + \gamma + 1) &\equiv \delta + 1 + \gamma',
\end{aligned}$$

conclut

$$\begin{aligned}
(0.0) &= (2.0), & (0.1) &= (1.3), & (0.3) &= (3.1), \\
(1.0) &= (1.1) = (2.1).
\end{aligned}$$

ite de ces onze relations, le schéma S prend cette forme

$$\begin{array}{cccc}
h & j & k & l \\
m & m & l & j \\
h & m & h & m \\
m & l & j & m.
\end{array}$$

-1 entre dans le groupe C, donc 0 dans C', on trouve  
 t de la même manière qu'au n° 8

$$h + j + k + l = \frac{\mu - 1}{4} = 2n + 1,$$

$$2m + l + j = 2n + 1,$$

$$h + m = n.$$

a considération du nombre des solutions de la congruence

$$\alpha + \beta + \gamma + 1 \equiv 0$$

core une relation entre  $h, j, k, l, m$ . Si l'on prend d'abord  
 tes les valeurs qui appartiennent à A, il arrive respecti

On trouve en outre, de la même manière qu'au n° 9, que pour chacun de ces cas la congruence a respectivement  $m, l, j, m$  solutions, de sorte que le nombre total des solutions est

$$hm + jl + kj + lm.$$

Prend-on, au contraire, d'abord pour  $\beta$  toutes les valeurs B, alors il arrive respectivement  $m, m, l, j$  fois que  $\beta + 1$  appartient aux groupes A, B, C, D. Pour chacun de ces cas, on trouve alors que la congruence a respectivement  $h, m, h, m$  solutions, ce qui donne pour le nombre total des solutions

$$mh + mm + lh + jm.$$

14. Egalons maintenant entre elles les deux expressions trouvées pour le nombre des solutions de la congruence

$$a + \beta + \gamma + 1 \equiv 0 \pmod{M};$$

il vient

$$0 = m^2 + lh + jm - jl - kj - lm,$$

ou, à cause de la valeur  $k = 2m - h$ , qui résulte immédiatement des relations linéaires établies entre  $h, j, k, l, m$  au n° 13,

$$0 = m^2 + lh + hj - jl - jm - lm.$$

A l'aide de  $j + l = 1 + 2h$ , on peut exprimer  $j$  et  $l$  en fonction de leur différence, ce qui donne

$$2j = 1 + 2h + (j - l),$$

$$2l = 1 + 2h - (j - l),$$

et par l'introduction de ces valeurs dans l'équation précédente, celle-ci se transforme en

$$0 = 4m^2 - 4m - 1 + 4h^2 - 8hm + (j - l)^2,$$

ou, à cause de

$$4m = 2(h + m) - 2(h - m) = 2n - 2(h - m),$$

on

$$0 = 4(h - m)^2 - 2n + 2(h - m) - 1 + (j - l)^2$$

et finalement en

$$\mu = 8n + 5 = [4(h - m) + 1]^2 + 4(j - l)^2;$$



$$A = 4(h - m) + 1, \quad B = 2j - 2l,$$

onc

$$\mu = A^2 + B^2.$$

moyen de A et B il est maintenant facile d'exprimer  $h, j, k$ ,  
e la manière suivante

$$8h = 4n + A - 1,$$

$$8j = 4n + A + 2B - 3,$$

$$8k = 4n - 3A + 3,$$

$$8l = 4n + A - 2B + 3,$$

$$8m = 4n - A + 1.$$

e encore à déterminer A et B. Or  $\mu$ , nombre premier réel  
orme  $4n + 1$ , ne peut être représenté que d'une seule manière  
somme de deux carrés, et comme

$$M = a + bi$$

$$\mu = a^2 + b^2,$$

$$a \equiv -1, \quad b \equiv 2 \pmod{4}.$$

à résulte donc

$$A = -a \text{ et } B = \pm b.$$

igne de B s'obtient par une considération analogue à celle  
2.

rouve aisément

$$\Sigma(z^2 + 1)^{\frac{\mu-1}{4}} \equiv -1 \equiv 2(h - k) + 2i(j - l) \pmod{M}.$$

$$2(h - k) = A - 1, \quad 2(j - l) = B,$$

$$-1 \equiv A - 1 + Bi,$$

$$0 \equiv A + Bi \pmod{M = a + bi}.$$

u'on a déjà trouvé  $A = -a$ , il s'ensuit  $B = -b$ , de sorte  
 finalement

$$8h = 4n - a - 1,$$

$$8j = 4n - a - 2b + 3,$$

$$8k = 4n + 3a + 3,$$

$$8l = 4n - a + 2b + 3,$$

$$8m = 4n + a + 1.$$

$\mu = 8n + 1$  le schéma S est de la forme

$$\begin{array}{cccc} h & j & k & l \\ j & l & m & m \\ k & m & k & m \\ l & m & m & j \end{array}$$

Ainsi on trouve

$$\begin{array}{ll} \text{pour } M = -q & \begin{array}{l} 8h = 4n - 3M - 5, \\ 8j = 8k = 8l = 4n + M - 1, \\ 8m = 4n - M + 1; \end{array} \\ \text{pour } M = a + bi & \begin{array}{l} 8h = 4n - 3a - 5, \\ 8j = 4n + a - 2b - 1, \\ 8k = 4n + a - 1, \\ 8l = 4n + a + 2b - 1, \\ 8m = 4n - a + 1. \end{array} \end{array}$$

Pour  $\mu = 8n + 5$ ,  $M = a + bi$ , le schéma S a la forme

$$\begin{array}{cccc} h & j & k & l \\ m & m & l & j \\ h & m & h & m \\ m & l & j & m \end{array}$$

de sorte qu'on a

$$\begin{array}{l} 8h = 4n - a - 1, \\ 8j = 4n - a - 2b + 3, \\ 8k = 4n + 3a + 3, \\ 8l = 4n - a + 2b + 3, \\ 8m = 4n + a + 1. \end{array}$$

Ainsi qu'il ressort de ces formules, le changement de correspond à une permutation de  $j$  et  $l$ , tant dans le cas de  $\mu = 8n + 1$  que lorsque  $\mu = 8n + 5$ .

D'après les congruences du n<sup>o</sup> 5, on a, dans le cas  $\mu = 8n + 1$  pour le caractère de  $1 + i$  suivant le module 4

$$(3.1) + 2(3.2) + 3(3.3) = 3m + 3j \equiv -m - j,$$

et pour celui de  $1 - i$

$$(1.1) + 2(1.2) + 3(1.3) = l + 5m \equiv l + m,$$

donc, pour  $M = -q$ , il suit

$$\text{Caractère } (1+i) \equiv -n = -\frac{q^2-1}{8},$$

$$\text{Caractère } (1-i) \equiv n = \frac{q^2-1}{8}.$$

Or,  $\frac{q+1}{4}$  et  $\frac{q-3}{4}$  sont des nombres entiers consécutifs; le produit est donc pair et  $\frac{(q+1)(q-3)}{8}$  est divisible par 4, d'où qu'on a

$$\frac{q^2-1}{8} \equiv \frac{q^2-1}{8} - \frac{(q+1)(q-3)}{8} = \frac{q+1}{4},$$

par conséquent

$$\left(\left(\frac{1+i}{M}\right)\right) = i^{\frac{M-1}{4}}, \quad \left(\left(\frac{1-i}{M}\right)\right) = i^{-\frac{M-1}{4}},$$

et, vu que  $-1$  est résidu biquadratique,

$$\left(\left(\frac{-1-i}{M}\right)\right) = i^{\frac{M-1}{4}}, \quad \left(\left(\frac{-1+i}{M}\right)\right) = i^{-\frac{M-1}{4}},$$

tandis que, de  $2 = (1-i)(1+i)$ , il suit encore

$$\left(\left(\frac{2}{M}\right)\right) = \left(\left(\frac{-2}{M}\right)\right) = 1.$$

Pour  $M = a + bi$ , au contraire, on a

$$-m-j = -n + \frac{1}{4}b,$$

$$l+m = n + \frac{1}{4}b$$

et

$$n = \frac{a^2 + b^2 - 1}{8}.$$

Mais évidemment  $\frac{a-1}{4} \cdot \frac{a+3}{4}$  est pair, et par conséquent  $\frac{(a-1)(a+3)}{8}$  est divisible par 4, d'où il suit

$$a^2 - 1 \equiv -a + 1 \pmod{4}$$

visible par 8;  $\frac{b(b-4)}{8}$  est donc divisible par 4 et on a

$$\frac{b^2}{8} \equiv \frac{b^2}{8} - \frac{b(b-4)}{8} = \pm \frac{1}{2}b,$$

de sorte que

$$n \equiv \frac{1}{4}(-a+1 \pm 2b) \pmod{4}$$

et finalement

$$\left(\left(\frac{1+i}{M}\right)\right) = \left(\left(\frac{-1-i}{M}\right)\right) = i^{\frac{a-1-b}{4}},$$

$$\left(\left(\frac{1-i}{M}\right)\right) = \left(\left(\frac{-1+i}{M}\right)\right) = i^{\frac{-a+1-b}{4}},$$

$$\left(\left(\frac{2}{M}\right)\right) = i^{-\frac{b}{2}}.$$

Lorsque, enfin,  $\mu = 8n + 5$ ,  $M = a + bi$ , on a

$$\text{Caractère } (1+i) \equiv (1.1) + 2(1.2) + 3(1.3) = m + 2l + 3j \pmod{4}$$

$$\text{Caractère } (1-i) \equiv (3.1) + 2(3.2) + 3(3.3) = l + 2j + 3m \pmod{4}$$

où, toutes les congruences ayant rapport au module 4, on a

$$m + 2l + 3j = 3n + \frac{1}{4}(-2a - b + 8),$$

$$l + 2j + 3m = 3n + \frac{1}{4}(-b + 6) \equiv -n + \frac{1}{4}(-b + 6),$$

$$n = \frac{a^2 + b^2 - 5}{8};$$

le produit  $\frac{a-3}{4} \cdot \frac{a+1}{4}$  étant pair,  $\frac{(a-3)(a+1)}{8}$  est divisible par 4

et il en est de même de  $\frac{(b-2)(b+2)}{8}$ ; donc

$$n \equiv \frac{a^2 + b^2 - 5}{8} - \frac{(a-3)(a+1)}{8} - \frac{b^2 - 4}{8} = \frac{1}{4}(a+1),$$

de sorte qu'on obtient finalement

$$m + 2l + 3j \equiv \frac{1}{4}(a - b + 11) \equiv (a - b - 5),$$

$$l + 2j + 3m \equiv \frac{1}{4}(-a - b + 5),$$

par suite

$$\left(\left(\frac{1+i}{a+bi}\right)\right) = i^{\frac{a-b-5}{4}}, \quad \left(\left(\frac{1-i}{a+bi}\right)\right) = i^{\frac{-a-b+5}{4}}$$

$$\left(\left(\frac{-1-i}{a+bi}\right)\right) = i^{\frac{a-b+3}{4}}, \quad \left(\left(\frac{-1+i}{a+bi}\right)\right) = i^{-\frac{a-b-3}{4}},$$

$$\left(\left(\frac{2}{a+bi}\right)\right) = i^{-\frac{b}{2}}.$$

Par là se trouve déterminé, dans chaque cas, le caractère biquadratique de  $1+i$ , ainsi que celui de  $1-i$ ,  $-1-i$ ,  $-1+i$ , par rapport à un nombre premier primaire. Les résultats concordent entièrement avec ceux donnés par Gauss dans les art. 63, 64 de la *Theoria residuorum biquadraticorum commentatio secunda* et démontrés par lui, d'une manière tout à fait différente, dans les art. 68—76.

16. Relativement à l'analogie qui existe entre une grande partie des considérations précédentes et celles que Gauss a développées dans les art. 8 et suiv. de son premier mémoire sur la théorie des résidus biquadratiques, il y a à faire les remarques suivantes :

Gauss considère des nombres réels; le module premier  $p$  est de la forme  $4n+1$ , et il faut distinguer les deux cas  $p=8n+1$ ,  $p=8n+5$ ;  $p$  a donc la même signification que la norme  $\mu$  dans les cas II et III de notre n<sup>o</sup> 4.

Les nombres  $1, 2, 3, \dots, p-1$  sont partagés par Gauss en 4 classes A, B, C, D. Les nombres de ces classes étant représentés par  $\alpha, \beta, \gamma, \delta$ , cette classification est fondée sur les congruences

$$\begin{aligned} \alpha^{\frac{\mu-1}{4}} &\equiv 1 \\ \beta^{\frac{\mu-1}{4}} &\equiv f \\ \gamma^{\frac{\mu-1}{4}} &\equiv -1 \\ \delta^{\frac{\mu-1}{4}} &\equiv -f \end{aligned} \quad (\text{mod } \mu = p),$$

où  $f^2 \equiv -1 \pmod{p}$ , et pour  $\mu = a^2 + b^2$

$$a \equiv 1 \pmod{4}, \quad a + bf \equiv 0 \pmod{p}.$$

Pour  $p = \mu = 8n+1$ ,  $a$  et  $b$  ont la même signification que ci-dessus; pour  $p = 8n+5$ ,  $a$  et  $b$ , chez Gauss, ne diffèrent que par le signe

nombre premier complexe primaire.

Lorsque, toutefois, on admet aussi des nombres complexes, il est clair que les congruences ci-dessus, qui sont relatives au module  $p = \mu$ , restent valables pour le module  $a + bi$ , de sorte qu'on a aussi  $a + bf \equiv 0 \pmod{a + bi}$ , d'où résulte  $f \equiv i \pmod{a + bi}$ , et par conséquent

$$a^{\frac{\mu-1}{4}} \equiv 1, \beta^{\frac{\mu-1}{4}} \equiv i, \gamma^{\frac{\mu-1}{4}} \equiv -1, \delta^{\frac{\mu-1}{4}} \equiv -i \pmod{a + bi}.$$

La classification de Gauss est donc identique à celle établie suivant le caractère biquadratique 0, 1, 2, 3 par rapport au module  $a + bi$ .

Effectivement, les nombres réels 1, 2, 3, ...,  $p-1$  forment pour le module  $a + bi$  un système complet de résidus incongrus entre eux non divisibles par le module.

Aussi, en remplaçant dans les deux derniers exemples du n° 4 les résidus complexes par les nombres réels congrus, ce qui se fait sans peine à l'aide de  $i \equiv 27 \pmod{-3 - 8i}$  et  $i \equiv 11 \pmod{-5 + 6i}$ , on obtient

$$\pmod{-3 - 8i}, \quad \mu = 73,$$

A 1, 2, 4, 8, 9, 16, 18, 32, 36, 37, 41, 55, 57, 64, 65, 69, 71, 72

B 5, 7, 10, 14, 17, 20, 28, 33, 34, 39, 40, 45, 53, 56, 59, 63, 66, 68

C 3, 6, 12, 19, 23, 24, 25, 27, 35, 38, 46, 48, 49, 50, 54, 61, 67, 70

D 11, 13, 15, 21, 22, 26, 29, 30, 31, 42, 43, 44, 47, 51, 52, 58, 60, 62

$$\pmod{-5 + 6i}, \quad \mu = 61,$$

A 1, 9, 12, 13, 15, 16, 20, 22, 25, 34, 42, 47, 56, 57, 58.

B 2, 7, 18, 23, 24, 26, 30, 32, 33, 40, 44, 50, 51, 53, 55.

C 3, 4, 5, 14, 19, 27, 36, 39, 41, 45, 46, 48, 49, 52, 60.

D 6, 8, 10, 11, 17, 21, 28, 29, 31, 35, 37, 38, 43, 54, 59,

en accord parfait avec les exemples donnés par Gauss dans l'art 1 de son premier mémoire.

Le cas I de notre n° 4 est le seul pour lequel il n'existe rien d'analogue dans la théorie réelle de Gauss, ce qui tient à ce que dans ce cas on ne peut pas former, avec des nombres réels, un système complet de résidus.

tuee par Gauss dans son premier mémoire, est identique à celle faite d'après le caractère biquadratique par rapport au module  $a + bi$  fournit aussi le moyen de déduire immédiatement tous les théorèmes que Gauss a trouvés par induction dans son second mémoire, art. 28 mais dont, à ma connaissance, aucune démonstration n'a encore été donnée jusqu'ici.

Ces théorèmes sont relatifs à la présence d'un nombre premier réel  $m$  dans les quatre classes A, B, C, D, ou, d'après ce qui précède, au caractère biquadratique de  $m$  par rapport au module  $a + bi$ .

17. Je vais reproduire maintenant les remarques formulées par Gauss dans l'art. 28. Le module premier  $p = \mu$  étant supposé de la forme  $4n + 1$ , il s'agit maintenant, d'après ce qui a été dit au n° précédent, de déterminer la valeur du symbole

$$\left( \left( \frac{m}{a + bi} \right) \right),$$

où  $m$  est un nombre premier réel; la circonstance que, pour  $\mu = 8n + 5$ ,  $a$  et  $b$  ont chez Gauss un signe différent de celui des valeurs du n° 14, n'a aucune influence sur l'énoncé des théorèmes. Le nombre premier  $m$  recevra un signe tel qu'il soit toujours  $\equiv 1 \pmod{4}$ , donc le signe *moins* lorsque, pris positivement, il est de la forme  $4k + 3 = Q$ ; quant à un nombre premier positif de la forme  $4k + 1$ , il sera représenté par P. Les remarques de Gauss peuvent alors être exprimées de cette manière:

I. Lorsque  $a \equiv 0 \pmod{m}$ , la valeur de  $\left( \left( \frac{m}{a + bi} \right) \right)$  est  $+1$  ou  $-1$ ; elle est égale à  $+1$  si  $m$  a la forme  $8r \pm 1$ , égale à  $-1$  si  $m$  a la forme  $8r \pm 3$ .

II. Lorsque  $a$  n'est pas divisible par  $m$ , la valeur du symbole dépend uniquement du nombre complètement déterminé  $x$ , qui satisfait à

$$b \equiv ax \pmod{m}.$$

Pour  $m = P$ ,  $x$  peut prendre ici les valeurs suivantes

$$0, 1, 2, 3, \dots, P - 1,$$

à l'exception des deux valeurs  $f$  et  $P - f$  qui satisfont à  $yy \equiv -1 \pmod{P}$ . Ces deux valeurs ne peuvent évidemment pas se présenter car de  $b \equiv ay$  il résulterait

$$b^2 \equiv -a^2 \text{ ou } a^2 + b^2 \equiv p \equiv 0 \pmod{P},$$

c'est-à-dire que  $p$  devrait être divisible par  $P$ .

Pour  $m = -Q$ , au contraire,  $x$  peut prendre toutes les valeurs

$$0, 1, 2, 3, \dots, Q - 1.$$

Ces valeurs de  $x$  peuvent être réparties en 4 classes  $\alpha, \beta, \gamma, \delta$ , de telle sorte que, pour

$$b \equiv a \alpha \pmod{m} \text{ la valeur du symbole soit } = 1,$$

$$b \equiv a \beta \quad " \quad " \quad " \quad " \quad " \quad " = i,$$

$$b \equiv a \gamma \quad " \quad " \quad " \quad " \quad " \quad " = -1,$$

$$b \equiv a \delta \quad " \quad " \quad " \quad " \quad " \quad " = -i,$$

ou, ce qui revient au même, que dans ces cas  $m$  appartienne respectivement aux classes A, B, C, D.

Or, en ce qui concerne la quotité des nombres  $\alpha, \beta, \gamma, \delta$ , existe cette règle: que 3 de ces quotités sont égales, tandis que la quatrième est plus petite d'une unité; d'ailleurs, cette quatrième quotité est celle des  $\alpha$  lorsque, pour  $a \equiv 0$ ,  $m$  appartient à A, et celle des  $\gamma$  lorsque pour  $a \equiv 0$ ,  $m$  appartient à C.

18. Soit donc, en premier lieu,  $m = -Q$ ; d'après la loi de réciprocité, on a alors

$$\left( \left( \frac{-Q}{a + bi} \right) \right) = \left( \left( \frac{a + bi}{Q} \right) \right)$$

et pour  $a \equiv 0 \pmod{Q}$

$$\left( \left( \frac{-Q}{a + bi} \right) \right) = \left( \left( \frac{bi}{Q} \right) \right) = \left( \left( \frac{b}{Q} \right) \right) \left( \left( \frac{i}{Q} \right) \right) = i^{\frac{Q^2-1}{4}},$$

vu que  $\left( \left( \frac{b}{Q} \right) \right) = 1$ ; en effet, on a

$$\left( \left( \frac{b}{Q} \right) \right) \equiv b^{\frac{Q^2-1}{4}} \pmod{Q}$$

et comme  $Q$  est de la forme  $4r + 3$ , donc  $\frac{Q^2-1}{4} = (Q-1) \frac{Q+1}{4}$  un multiple de  $Q-1$ , il suit du théorème de Fermat



$$\left(\left(\frac{-Q}{a+bi}\right)\right) = -1,$$

pour  $Q = 8n + 7$

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = +1.$$

Lorsque, au contraire, on a  $m = P = (A + Bi)(A - Bi)$  ou  $A + Bi$  et  $A - Bi$  sont les facteurs primaires de  $P$ , il suit de la loi de réciprocité

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{A+Bi}\right)\right) \left(\left(\frac{a+bi}{A-Bi}\right)\right)$$

et pour  $a \equiv 0 \pmod{P}$

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{bi}{A+Bi}\right)\right) \left(\left(\frac{bi}{A-Bi}\right)\right) = \left(\left(\frac{-bi}{A+Bi}\right)\right) \left(\left(\frac{+bi}{A-Bi}\right)\right) \left(\left(\frac{-1}{A+Bi}\right)\right)$$

Or, en général, comme l'on sait,

$$\left(\left(\frac{a+\beta i}{A+Bi}\right)\right) \left(\left(\frac{a-\beta i}{A-Bi}\right)\right) = 1,$$

donc

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{-1}{A+Bi}\right)\right) = (-1)^{\frac{P-1}{4}},$$

ou, pour  $P = 8n + 1$

$$\left(\left(\frac{P}{a+bi}\right)\right) = 1$$

et pour  $P = 8n + 5$

$$\left(\left(\frac{P}{a+bi}\right)\right) = -1.$$

Ainsi se trouve complètement démontrée la proposition énoncée au n° précédent, sous I.

19. Supposons maintenant que  $a$  ne soit pas divisible par  $m$ , considérons d'abord le cas le plus simple

$$m = -Q,$$

on a donc alors

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{a+bi}{Q}\right)\right)$$

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{a(1+xi)}{Q}\right)\right) = \left(\left(\frac{1+xi}{Q}\right)\right),$$

cause de l'égalité  $\left(\left(\frac{a}{Q}\right)\right) = 1$ , déjà démontrée au n<sup>o</sup> précédent.

Du résultat obtenu

$$\left(\left(\frac{-Q}{a+bi}\right)\right) = \left(\left(\frac{1+xi}{Q}\right)\right)$$

il ressort déjà que la valeur du symbole à gauche dépend uniquement du nombre  $x$ , lequel peut prendre les  $Q$  valeurs

$$0, 1, 2, 3, \dots, Q-1.$$

Nous n'avons donc plus qu'à résoudre cette question: lorsque  $Q$  module  $Q$  est un nombre premier de la forme  $4n+3$ , combien y a-t-il parmi les nombres

$$1, 1+i, 1+2i, 1+3i, \dots, 1+(Q-1)i,$$

qui appartiennent respectivement aux classes A, B, C, D.

A cet effet, je remarquerai, en premier lieu, qu'on peut prendre comme système complet de résidus non divisibles par  $Q$ , les nombres

$$a + \beta i$$

où  $a$  et  $\beta$  parcourent les valeurs  $0, 1, 2, 3, \dots, Q-1$ , à l'exception de la combinaison  $a=0, \beta=0$ ; et, en second lieu, que les nombres

$$1, 2, 3, \dots, Q-1$$

appartiennent tous à A, de sorte que, lorsque le nombre

$$\alpha' + \beta' i$$

fait partie d'une certaine classe, celle-ci renferme également les nombres

$$2(\alpha' + \beta' i), 3(\alpha' + \beta' i), \dots, (Q-1)(\alpha' + \beta' i)$$

qui, par l'omission de multiples de  $Q$ , peuvent tous être ramenés à la forme  $a + \beta i$  où  $a$  et  $\beta$  sont plus petits que  $Q$ . Or, les résidus d

$$\alpha', 2\alpha', 3\alpha', \dots, (Q-1)\alpha',$$

sont, tant que  $\alpha'$  n'est pas zéro, congrus dans un certain ordre suivant le module  $Q$ , aux nombres

$$1, 2, 3, \dots, Q-1.$$

$$\alpha' + \beta' i, 2(\alpha' + \beta' i), \dots, (Q-1)(\alpha' + \beta' i),$$

appartenant tous à la même classe, il y en a donc un qui est congru à un des nombres

$$1 + xi \quad (x=0, 1, 2, \dots, Q-1).$$

Or, la quotité des nombres de chaque classe,

$$\frac{Q^2-1}{4} = (Q-1) \times \frac{Q+1}{4},$$

est un multiple de  $Q-1$ , et les  $Q-1$  nombres sans partie réelle

$$i, 2i, 3i, \dots, (Q-1)i$$

appartiennent pour  $Q=8n+7$  à A, pour  $Q=8n+3$  à C.

Puisque tous les nombres de chaque classe dont la partie réelle n'est pas zéro peuvent être réunis, comme ci-dessus, en groupes de  $Q-1$  nombres, de telle sorte que dans chaque groupe il y ait un nombre à partie réelle égale à 1, il en résulte que, pour  $Q=8n+7$  il y a dans les classes A, B, C, D respectivement

$$\frac{Q-3}{4}, \quad \frac{Q+1}{4}, \quad \frac{Q+1}{4}, \quad \frac{Q+1}{4}$$

nombres  $1 + xi$ .

Pour  $Q=8n+3$ , ces nombres sont

$$\frac{Q+1}{4}, \quad \frac{Q+1}{4}, \quad \frac{Q-3}{4}, \quad \frac{Q+1}{4},$$

tandis que, d'après le n° 18, dans le cas  $a \equiv 0 \pmod{Q}$ , pour  $Q=8n+7$  et  $8n+3$ ,  $Q$  appartenait respectivement aux classes A et C.

Tout ce qui se rapportait au cas  $m = -Q$  est donc maintenant connu.

20. Pour  $m = P = (A + Bi)(A - Bi)$  nous avons déjà trouvé

$$\left( \left( \frac{P}{a + bi} \right) \right) = \left( \left( \frac{a + bi}{A + Bi} \right) \right) \quad \left( \left( \frac{a + bi}{A - Bi} \right) \right)$$

et par conséquent, lorsque

$$b \equiv ax \pmod{P},$$

$$\left( \left( \frac{P}{a + bi} \right) \right) = \left( \left( \frac{1 + xi}{A + Bi} \right) \right) \quad \left( \left( \frac{1 + xi}{A - Bi} \right) \right) \quad \left( \left( \frac{a}{A + Bi} \right) \right) \quad \left( \left( \frac{a}{A - Bi} \right) \right)$$

deux derniers facteurs à droite est égal à 1,

$$\left(\left(\frac{P}{a+bi}\right)\right) = \left(\left(\frac{1+xi}{A+Bi}\right)\right) \left(\left(\frac{1+xi}{A-Bi}\right)\right);$$

de là résulte que la valeur du symbole à gauche dépend uniquement du nombre  $x$ , de sorte qu'il n'y a plus qu'à résoudre la question suivante: pour combien de valeurs de  $1+xi$  l'expression

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right) \left(\left(\frac{1+xi}{A-Bi}\right)\right)$$

acquiert-elle respectivement les valeurs 1,  $i$ ,  $-1$ ,  $-i$ ? On doit donner ici à  $x$  les valeurs

$$0, 1, 2, 3, \dots, P-1$$

à l'exception des deux racines de  $y^2 \equiv -1 \pmod{P}$ .

Pour résoudre la question qui vient d'être posée, je considère un système complet de résidus incongrus non divisibles par le module  $A+Bi$ , et je les rapporte, d'après leur caractère biquadratique à 4 groupes A, B, C, D. Chacun de ces résidus est supposé choisi de telle sorte que la partie réelle soit égale à 1, et que le facteur de  $i$  soit plus petit que P.

Ces suppositions peuvent être représentées ainsi

	$(\text{mod } A+Bi), \quad A^2+B^2=P.$
Classe A	$\alpha = 1 + a i$
B	$\beta = 1 + b i$
C	$\gamma = 1 + c i$
D	$\delta = 1 + d i$

Les nombres  $a, b, c, d$ , dans leur ensemble, concordent avec

$$0, 1, 2, 3, \dots, (P-1),$$

sauf que la valeur  $f$ , qui est  $\equiv i$ , manque, vu que  $1+fi \equiv 0 \pmod{A+Bi}$ .

En opérant de la même manière avec  $A-Bi$ , on voit aisément que la classification sera

	$(\text{mod } A-Bi), \quad A^2+B^2=P.$
Classe A	$1 + (P-a) i$
B	$1 + (P-d) i$
C	$1 + (P-c) i$
D	$1 + (P-b) i$

$$(1 + xi)^{\frac{P-1}{4}} - i^p = (A + Bi)(C + Di),$$

$$(1 - xi)^{\frac{P-1}{4}} - i^{3p} = (A - Bi)(C - Di).$$

Ainsi, lorsque  $1 + xi$  a, suivant le module  $A + Bi$ , le caractère  $g$   
 $1 - xi \equiv 1 + (P - x)i$  a, suivant le module  $A - Bi$ , le caractère  $3g$

21. Pour que

$$\left( \left( \frac{1 + xi}{A + Bi} \right) \right) \left( \left( \frac{1 + xi}{A - Bi} \right) \right)$$

devienne égal à 1, il faut, lorsque

$$\left( \left( \frac{1 + xi}{A + Bi} \right) \right)$$

a l'une des valeurs 1,  $i$ ,  $-1$ ,  $-i$ , que

$$\left( \left( \frac{1 + xi}{A - Bi} \right) \right)$$

prenne une des valeurs 1,  $i$ ,  $-1$ ,  $-i$ ; ou, en ayant égard aux  
deux divisions en classes: lorsque  $x$  appartient respectivement à  
 $a, b, c, d$ , il faut que, simultanément,  $P - x$  appartienne aux nombre  
 $a, b, c, d$ .

On peut donc dire que le nombre des valeurs de  $x$  pour lesquelles  
on a

$$\left( \left( \frac{1 + xi}{A + Bi} \right) \right) \left( \left( \frac{1 + xi}{A - Bi} \right) \right) = 1$$

est égal à la somme des nombres de solutions des congruences

$$a + a' \equiv 0,$$

$$b + b' \equiv 0,$$

$$c + c' \equiv 0,$$

$$d + d' \equiv 0,$$

par rapport au module  $P$ , ou, ce qui revient au même, par rapport  
au module  $A + Bi$ .

On remarquera que la valeur  $P - f$ , exclue pour  $x$ , entre bien  
dans  $a, b, c, d$ , mais ne peut néanmoins apparaître dans aucune de  
congruences ci dessus, parce que cela exigerait que  $f$  se trouvât  
également parmi les nombres  $a, b, c, d$ , ce qui n'est pas le cas.

multiplication par  $i$ , deviennent

$$\begin{aligned}\alpha + \alpha' &\equiv 2 \\ \beta + \beta' &\equiv 2 \\ \gamma + \gamma' &\equiv 2 \\ \delta + \delta' &\equiv 2\end{aligned} \pmod{A + Bi}.$$

Lorsque  $\frac{P-1}{2}$  appartient à la classe A, les congruences précédentes, multipliées par  $\frac{P-1}{2}$ , se transforment en

$$\begin{aligned}\alpha + \alpha' + 1 &\equiv 0 \\ \beta + \beta' + 1 &\equiv 0 \\ \gamma + \gamma' + 1 &\equiv 0 \\ \delta + \delta' + 1 &\equiv 0\end{aligned} \pmod{A + Bi},$$

de sorte que la somme des nombres de solutions de ces congruences est égale au nombre des valeurs de  $x$  qui rendent

$$\left(\left(\frac{1+xi}{A+Bi}\right)\right) \left(\left(\frac{1+xi}{A-Bi}\right)\right)$$

égal à 1.

Mais on peut se convaincre immédiatement que ce résultat reste le même lorsque  $\frac{P-1}{2}$  appartient aux classes B, C, D. Si, par exemple,  $\frac{P-1}{2}$  appartient à B, il suit de  $\alpha + \alpha' \equiv 2$ , en multipliant par  $\frac{P-1}{2}$ ,

$$\beta + \beta' + 1 \equiv 0,$$

et de  $\beta + \beta' \equiv \gamma + \gamma' \equiv \delta + \delta' \equiv 2$ , respectivement

$$\gamma + \gamma' + 1 \equiv 0, \quad \delta + \delta' + 1 \equiv 0, \quad \alpha + \alpha' + 1 \equiv 0.$$

Si l'on désigne par  $t, u, v, w$ , les nombres des valeurs de  $x$  qui rendent  $\left(\left(\frac{1+xi}{A+Bi}\right)\right) \left(\left(\frac{1+xi}{A-Bi}\right)\right)$  respectivement égal à 1,  $i$ ,  $-1$ ,  $-i$ ,  $t$  est donc la somme des nombres de solutions des congruences

$$\begin{aligned}\alpha + \alpha' + 1 &\equiv 0 \\ \beta + \beta' + 1 &\equiv 0 \\ \gamma + \gamma' + 1 &\equiv 0 \\ \delta + \delta' + 1 &\equiv 0\end{aligned} \pmod{A + Bi}.$$

des nombres de solutions des congruences

$$\alpha + \delta + 1 \equiv 0,$$

$$\beta + \alpha + 1 \equiv 0,$$

$$\gamma + \beta + 1 \equiv 0,$$

$$\delta + \gamma + 1 \equiv 0,$$

tandis que, pour  $v$  et  $w$ , on a à considérer les congruences

$$\alpha + \gamma + 1 \equiv 0,$$

$$\alpha + \beta + 1 \equiv 0,$$

$$\beta + \delta + 1 \equiv 0,$$

$$\beta + \gamma + 1 \equiv 0,$$

$$\gamma + \alpha + 1 \equiv 0,$$

$$\gamma + \delta + 1 \equiv 0,$$

$$\delta + \beta + 1 \equiv 0,$$

$$\delta + \alpha + 1 \equiv 0,$$

Dans le cas de  $P = 8n + 1$  on a donc, d'après les  $n^0$  7, 8

$$t = (0.0) + (1.1) + (2.2) + (3.3) = h + l + k + j = 2n - 1,$$

$$u = (0.3) + (1.0) + (2.1) + (3.2) = l + j + m + m = 2n,$$

$$v = (0.2) + (1.3) + (2.0) + (3.1) = k + m + k + m = 2n,$$

$$w = (0.1) + (1.2) + (2.3) + (3.0) = j + m + m + l = 2n,$$

et dans le cas de  $P = 8n + 5$ , d'après le  $n^0$  13

$$t = (0.2) + (1.3) + (2.0) + (3.1) = k + j + h + l = 2n + 1,$$

$$u = (0.1) + (1.2) + (2.3) + (3.0) = j + l + m + m = 2n + 1,$$

$$v = (0.0) + (1.1) + (2.2) + (3.3) = h + m + h + m = 2n,$$

$$w = (0.3) + (1.0) + (2.1) + (3.2) = l + m + m + j = 2n + 1.$$

22. En récapitulant tout ce qui précède, on voit donc que les caractères servant à reconnaître si un nombre premier réel appartient aux classes A, B, C, D, lorsque le module  $P$  est de la forme  $4n + 1$  et que  $a + bi$  est un facteur complexe primaire de  $P$ , se laissent énoncer de la manière suivante.

Le nombre premier  $P = 8n + 1$  appartient à

A pour  $a \equiv 0, \quad b \equiv a\alpha$

Nombre des  $a = 2n - 1,$

B "  $b \equiv a\beta$

(mod  $P$ ). " "  $\beta = 2n,$

C "  $b \equiv a\gamma$

" "  $\gamma = 2n,$

D "  $b \equiv a\delta$

" "  $\delta = 2n.$

Le nombre premier  $P = 8n + 5$  appartient à

A pour  $b \equiv a\alpha$

Nombre des  $a = 2n + 1,$

B "  $b \equiv a\beta$

(mod  $P$ ). " "  $\beta = 2n + 1,$

C "  $b \equiv a\gamma, \quad a \equiv 0$

" "  $\gamma = 2n,$

D "  $b \equiv a\delta$

" "  $\delta = 2n + 1.$

Le nombre premier  $-Q = -(8n+3)$  appartient à

A	pour $b \equiv a \alpha$		Nombre des $\alpha = 2n+1$ ,
B	" $b \equiv a \beta$	(mod Q).	" " $\beta = 2n+1$ ,
C	" $b \equiv a \gamma$ , $a \equiv 0$		" " $\gamma = 2n$ ,
D	" $b \equiv a \delta$		" " $\delta = 2n+1$ .

Le nombre premier  $-Q = -(8n+7)$  appartient à

A	pour $b \equiv a \alpha$ , $a \equiv 0$		Nombre des $\alpha = 2n+1$ ,
B	" $b \equiv a \beta$	(mod Q).	" " $\beta = 2n+2$ ,
C	" $b \equiv a \gamma$		" " $\gamma = 2n+2$ ,
D	" $b \equiv a \delta$		" " $\delta = 2n+2$ .

Je citerai encore les remarques suivantes de Gauss (art. 28), dont la démonstration, après tout ce qui précède, n'offre pas la moindre difficulté.

1. Le nombre 0 appartient toujours aux  $a$ , et les nombres  $-\alpha$ ,  $-\beta$ ,  $-\gamma$ ,  $-\delta$ , appartiennent (mod  $m$ ) respectivement aux  $a$ ,  $\delta$ ,  $\gamma$  et  $\beta$ .

2. Pour  $P = 8n+1$ ,  $Q = 8n+7$ , les valeurs de  $\frac{1}{a}$ ,  $\frac{1}{\beta}$ ,  $\frac{1}{\gamma}$ ,  $\frac{1}{\delta}$  (mod  $m$ ) appartiennent respectivement aux  $a$ ,  $\delta$ ,  $\gamma$ ,  $\beta$ ; et pour  $P = 8n+5$ ,  $Q = 8n+3$ , ces valeurs appartiennent respectivement aux  $\gamma$ ,  $\beta$ ,  $a$ ,  $\delta$ .

## RÉSIDUS CUBIQUES.

23. En passant aux résidus cubiques, il est nécessaire de rappeler quelques points de la théorie des nombres entiers de la forme  $a + b\varrho$  où  $\varrho$  est ici une racine cubique complexe de l'unité, de sorte qu'on a  $1 + \varrho + \varrho^2 = 0$ .

Dans cette théorie, comme on le sait, il existe au sujet de la divisibilité des nombres, de leur décomposition en facteurs premiers, de l'existence de racines primitives des nombres premiers, etc., des théorèmes tout à fait analogues à ceux que présente la théorie ordinaire des nombres réels; la grande majorité des recherches contenues dans les quatre premières sections des *Disquisitiones arithmeticae* peuvent être étendues, presque sans changement, à la théorie



Le produit de deux nombres conjugués  $a + b\varrho$ ,  $a + b\varrho^2$ ,

$$(a + b\varrho)(a + b\varrho^2) = a^2 - ab + b^2$$

s'appelle la norme du nombre  $a + b\varrho$  et sera toujours indiqué par  $N$ .

Le nombre 3 n'est pas un nombre premier dans cette théorie, car

$$3 = (1 - \varrho)(1 - \varrho^2) = -\varrho^2(1 - \varrho)^2.$$

Comme nombres premiers, outre  $1 - \varrho$ , se présentent dans cette théorie :

premièrement les nombres premiers réels de la forme  $3n - 1$ ; la norme est alors  $= (3n - 1)^2$ ;

secondement les facteurs premiers complexes des nombres premiers réels de la forme  $3n + 1$ . Ce nombre premier réel est alors en même temps la norme du facteur premier complexe. On a, par exemple

$$7 = (2 + 3\varrho)(2 + 3\varrho^2) = (2 + 3\varrho)(-1 - 3\varrho).$$

Les nombres premiers  $2 + 3\varrho$ ,  $-1 - 3\varrho$  ont tous les deux le nombre 7 pour norme.

Dans chacun de ces deux cas la norme est donc de la forme  $3k + 1$ .

Ensuite, il suffit de considérer des nombres premiers primaires, ce mot étant pris ici dans la signification que lui donne Eisenstein (Journal de Crelle, 27, p. 301), de sorte que  $a + b\varrho$  sera dit primaire lorsque  $a + 1$  et  $b$  sont tous les deux divisibles par 3. Les nombres premiers réels de la forme  $3n - 1$  doivent donc être pris positifs pour être primaires.

Soit donc  $M$  un nombre premier primaire,  $\mu$  la norme de la forme  $3n + 1$ . Un système complet de résidus incongrus, non divisibles par le module  $M$ , se compose alors de  $\mu - 1 = 3n$  nombres. Ces nombres peuvent être rapportés à 3 classes, comprenant chacune  $n$  nombres, suivant que leur puissance  $\frac{\mu - 1}{3}$  est congrue, d'après le module  $M$ , à 1,  $\varrho$  ou  $\varrho^2$ . Cette distribution peut être représentée ainsi

A	$\alpha, \alpha', \alpha'', \dots$
B	$\beta, \beta', \beta'', \dots$

$$\alpha^{\frac{\mu-1}{3}} \equiv 1, \quad \beta^{\frac{\mu-1}{3}} \equiv \varrho, \quad \gamma^{\frac{\mu-1}{3}} \equiv \varrho^2 \pmod{M}.$$

Le caractère cubique des nombres  $\alpha, \alpha', \alpha'', \dots$  est 0, celui des nombres  $\beta, \beta', \dots$  est 1, celui des nombres  $\gamma, \gamma', \dots$  est 2.

Il sera d'ailleurs facile aussi de faire usage du symbole d'Eisenstein et d'écrire par conséquent

$$\left[ \frac{\alpha}{M} \right] = 1, \quad \left[ \frac{\beta}{M} \right] = \varrho, \quad \left[ \frac{\gamma}{M} \right] = \varrho^2.$$

Il s'agit maintenant, en premier lieu, de déterminer le caractère cubique de  $1 - \varrho$ , ou la valeur du symbole  $\left[ \frac{1 - \varrho}{M} \right]$ .

24. L'addition de l'unité à tous les nombres de A, B, C donne naissance aux 3 groupes de nombres A', B', C'

$$\begin{array}{lll} \text{A'} & \alpha + 1, & \alpha' + 1, \quad \alpha'' + 1, \dots \\ \text{B'} & \beta + 1, & \beta' + 1, \quad \beta'' + 1, \dots \\ \text{C'} & \gamma + 1, & \gamma' + 1, \quad \gamma'' + 1, \dots \end{array}$$

et je représente par (0.0), (0.1), (0.2) les quotités des nombres de A qui sont respectivement congrus à des nombres de A, B, C; par (1.0), (1.1), (1.2) les quotités des nombres de B' qui sont respectivement congrus à des nombres de A, B, C; enfin par (2.0), (2.1), (2.2) les quotités des nombres de C' qui sont respectivement congrus à des nombres de A, B, C.

Tous ces nombres peuvent être réunis dans le schéma S

$$\begin{array}{lll} (0.0) & (0.1) & (0.2) \\ (1.0) & (1.1) & (1.2) \\ (2.0) & (2.1) & (2.2) \end{array}$$

et avec la détermination de ces nombres est aussi trouvé immédiatement le caractère cubique de  $1 - \varrho$ . Car les congruences manifestement identiques

$$\begin{aligned} (x - \alpha)(x - \alpha')(x - \alpha'') \dots &\equiv x^{\frac{\mu-1}{3}} - 1 \\ (x - \beta)(x - \beta')(x - \beta'') \dots &\equiv x^{\frac{\mu-1}{3}} - \varrho \pmod{M} \\ (x - \gamma)(x - \gamma')(x - \gamma'') \dots &\equiv x^{\frac{\mu-1}{3}} - \varrho^2 \end{aligned}$$

donnent pour  $x \equiv -1$ , vu que  $\frac{1}{3}$  est pair (sauf pour  $M \equiv 2$ , qui doit être excepté)

$$\begin{aligned}(\beta + 1)(\beta' + 1)(\beta'' + 1) \dots &\equiv 1 - \varrho \\(\gamma + 1)(\gamma' + 1)(\gamma'' + 1) \dots &\equiv 1 - \varrho^2 \pmod{M},\end{aligned}$$

d'où il suit immédiatement

$$\begin{aligned}\left[\frac{1 - \varrho}{M}\right] &= \varrho^{(1,1) + 2(1,2)}, \\ \left[\frac{1 - \varrho^2}{M}\right] &= \varrho^{(2,1) + 2(2,2)}.\end{aligned}$$

25. Le nombre  $-1$  appartient, comme cube parfait, à la classe A, et les nombres  $\alpha$  et  $-\alpha$ ,  $\beta$  et  $-\beta$ ,  $\gamma$  et  $-\gamma$  entrent à la fois dans les classes A, B, C.

A l'aide de cette remarque, il est facile de voir que

le signe	représente le nombre des solutions de
(0.0)	$\alpha + \alpha' + 1 \equiv 0$
(0.1)	$\alpha + \beta + 1 \equiv 0$
(0.2)	$\alpha + \gamma + 1 \equiv 0$
(1.0)	$\beta + \alpha + 1 \equiv 0$
(1.1)	$\beta + \beta' + 1 \equiv 0 \pmod{M},$
(1.2)	$\beta + \gamma + 1 \equiv 0$
(2.0)	$\gamma + \alpha + 1 \equiv 0$
(2.1)	$\gamma + \beta + 1 \equiv 0$
(2.2)	$\gamma + \gamma' + 1 \equiv 0$

de sorte qu'on a

$$(0.1) = (1.0), \quad (0.2) = (2.0), \quad (1.2) = (2.1).$$

Si  $xy \equiv 1 \pmod{M}$  et que  $x$  appartienne à A, il est évident que  $y$  appartient également à A; mais lorsque  $x$  appartient à B ou à C,  $y$  appartient respectivement à C ou à B, ce qu'on peut exprimer en écrivant

$$\alpha \alpha' \equiv 1, \quad \beta \gamma \equiv 1 \pmod{M}.$$

De

$$\begin{aligned}\gamma(\alpha + \beta + 1) &\equiv \gamma' + 1 + \gamma, \\ \beta(\alpha + \gamma + 1) &\equiv \beta' + 1 + \beta,\end{aligned}$$

$$(0.1) = (2.2), \quad (0.2) = (1.1),$$

de sorte que le schéma S a cette forme

$$\begin{array}{ccc} h & j & k \\ j & k & l \\ k & l & j \end{array}$$

Comme  $-1$  appartient à  $A'$ , et par conséquent  $0$  à  $A'$ , mais que sauf ce nombre  $0$  de  $A'$ , tous les nombres de  $A'$ ,  $B'$ ,  $C'$  sont congrus à un nombre de  $A$ ,  $B$  ou  $C$ , on a

$$\begin{aligned} h + j + k &= n - 1, \\ j + k + l &= n. \end{aligned}$$

Enfin, la considération du nombre des solutions de la congruence

$$\alpha + \beta + \gamma + 1 \equiv 0 \pmod{M},$$

où  $\alpha$ ,  $\beta$ ,  $\gamma$  doivent être choisis respectivement dans les classes  $A$ ,  $B$ ,  $C$ , fournit encore une relation entre  $h$ ,  $j$ ,  $k$ ,  $l$ . En effet, si l'on prend d'abord pour  $\alpha$  les nombres de  $A$ , on obtient pour le nombre en question

$$hl + jj + kk.$$

En prenant, au contraire, pour  $\beta$  successivement tous les nombres de  $B$ , on trouve pour ce même nombre

$$jk + kl + lj$$

donc

$$0 = hl + jj + kk - jk - kl - lj.$$

26. En éliminant  $h$  de cette dernière équation, à l'aide de  $h = l - 1$ , on a

$$0 = l(l - 1) + jj + kk - jk - kl - lj,$$

équation qui, multipliée par 4, prend, à cause de

$$(j + k)^2 + 3(j - k)^2 = 4(jj + kk - jk),$$

la forme

$$0 = 4l^2 - 4l + (j + k)^2 + 3(j - k)^2 - 4l(k + j),$$

ou bien, en ayant égard à  $l = n - (j + k)$  et en multipliant par 9

$$36n = 36l^2 + 9(j + k)^2 + 27(j - k)^2 - 36l(j + k) + 36(j + k);$$

en même temps on a

$$24n = 24(j + k + l)$$

donc, par soustraction,

$$12n = 36l^2 + 9(j+k)^2 + 27(j-k)^2 - 36l(j+k) + 12(j+k) - 24l,$$

ou

$$12n + 4 = 4\mu = (6l - 3j - 3k - 2)^2 + 27(j-k)^2.$$

Si l'on pose

$$A = 6l - 3j - 3k - 2,$$

$$B = 3j - 3k,$$

on a donc

$$4\mu = A^2 + 3B^2,$$

et  $h, j, k, l$ , se laissent alors facilement exprimer au moyen de  $A$  et  $B$ , de la manière suivante

$$9h = 3n + A - 7,$$

$$18j = 6n - A + 3B - 2,$$

$$18k = 6n - A - 3B - 2,$$

$$9l = 3n + A + 2.$$

Il reste encore à déterminer  $A$  et  $B$ , et pour cela deux cas doivent être distingués.

27. Si, en premier lieu,  $M$  est réel et de la forme  $3n - 1$ , donc  $u = M^2$ , il suit de

$$4\mu = 4M^2 = A^2 + 3B^2,$$

que  $A$  est  $\equiv \pm 2M$ ,  $B = 0$ . Car, si  $B$  n'était pas zéro, on pourrait déterminer un nombre entier  $x$  de telle sorte que

$$A \equiv Bx \pmod{M},$$

d'où résulterait

$$A^2 \equiv -3B^2 \equiv B^2x^2 \pmod{M}$$

donc

$$x^2 \equiv -3 \pmod{M},$$

ce qui est impossible, puisqu'on sait que  $-3$  est non-résidu de  $M$ .

On a donc indubitablement  $B = 0$ ,  $A \equiv \pm 2M$ . Quant au signe de  $A$ , il se déduit immédiatement de la remarque que  $A$  est  $\equiv 1 \pmod{3}$  et  $M$ , comme nombre premier primaire,  $\equiv -1 \pmod{3}$ ; on a donc

$$A = 2M$$

et finalement

$$9h = 3n + 2M - 7,$$

$$9j = 9k = 3n - M - 1,$$

$$9l = 3n + 2M + 2.$$

naire d'un nombre premier réel  $p$  de la forme  $3n + 1$ ; on a alors

$$4\mu = (2a - b)^2 + 3b^2 = A^2 + 3B^2$$

et, puisque  $a + b\varrho$  est primaire,  $a + 1 \equiv b \equiv 0 \pmod{3}$ .

B aussi est maintenant divisible par 3, et comme il est facile de démontrer que  $4\mu$  ne peut être représenté que d'une seule manière par la somme d'un carré et du multiple par 27 d'un second carré, il s'ensuit

$$A = 2a - b, \quad B = \pm b.$$

Le signe de A, en effet est de nouveau déterminé par  $A \equiv 1 \pmod{3}$ . Quant au signe de B, il s'obtient par la considération suivante. Si  $z$  parcourt tous les nombres de A, B et C, on trouve, exactement de la même manière qu'au n° 12

$$\Sigma(z^3 + 1)^{\frac{\mu-1}{3}} \equiv -2 \equiv 3(h + j\varrho + k\varrho^2) \pmod{M},$$

ou

$$-2 \equiv 3[(h - k) + \varrho(j - k)]$$

puis, en exprimant  $h, j, k$  par A et B, et écrivant pour A la valeur  $2a - b$ , après quelques réductions

$$0 \equiv 2a - b + B + 2B\varrho \pmod{M = a + b\varrho},$$

d'où résulte  $B = b$ .

A et B étant ainsi trouvés, on a

$$9h = 3n + 2a - b - 7,$$

$$9j = 3n - a + 2b - 1,$$

$$9k = 3n - a - b - 1,$$

$$9l = 3n + 2a - b + 2.$$

29. D'après le n° 24, le caractère cubique de  $1 - \varrho$  suivant le module 3 est

$$(1.1) + 2(1.2) \equiv k - l,$$

et celui de  $1 - \varrho^2$

$$(2.1) + 2(2.2) \equiv l - j,$$

lorsque M est réel de la forme  $3n - 1$ , on a donc, d'après le n° 24

$$\text{Caractère}(1 - \varrho) \equiv -\frac{M + 1}{3},$$

$$\text{Caractère}(1 - \varrho^2) \equiv +\frac{M + 1}{3},$$

ou bien

$$\left[\frac{1-\varrho}{M}\right] = \varrho^{-\frac{M+1}{3}}, \quad \left[\frac{1-\varrho^2}{M}\right] = \varrho^{+\frac{M+1}{3}},$$

l'où il suit encore

$$\left[\frac{3}{M}\right] = 1.$$

Quand, au contraire,  $M = a + b\varrho$  est un facteur complexe d'un nombre premier réel de la forme  $3n + 1$ , on a, d'après les valeurs trouvées au n° 28

$$\text{Caractère } (1 - \varrho) \equiv -\frac{a+1}{3},$$

$$\text{Caractère } (1 - \varrho^2) \equiv \frac{a-b+1}{3},$$

ou

$$\left[\frac{1-\varrho}{a+b\varrho}\right] = \varrho^{-\frac{a+1}{3}}, \quad \left[\frac{1-\varrho^2}{a+b\varrho}\right] = \varrho^{\frac{a-b+1}{3}}, \quad \left[\frac{3}{a+b\varrho}\right] = \varrho^{-\frac{b}{3}}.$$

Ces résultats ne diffèrent pas, au fond, de ceux donnés par Eisenstein dans le tome 28 du Journal de Crelle, p. 28 et suiv.

30. A l'égard du cas où le nombre premier  $M$  est un facteur d'un nombre premier réel  $p$  de la forme  $3n + 1$ , je présenterai encore les remarques suivantes.

Comme, dans  $M = a + b\varrho$ ,  $a$  et  $b$  n'ont pas de diviseur commun et que par conséquent  $b$  et  $a - b$  sont aussi premiers entre eux, on peut toujours trouver deux nombres entiers  $\alpha$  et  $\beta$  satisfaisant à la relation

$$b\alpha + (a - b)\beta = 1$$

et on a alors

$$(a + b\varrho)(\alpha + \beta\varrho) = a\alpha - b\beta + \varrho,$$

donc

$$\varrho \equiv b\beta - a\alpha \pmod{M = a + b\varrho}.$$

De là résulte immédiatement que tout nombre entier  $c + d\varrho$  est congru suivant le module  $a + b\varrho$  à un nombre entier réel, lequel nombre réel peut être pris plus petit que le module  $\mu = p$ , de sorte que les nombres réels

$$0, 1, 2, 3, \dots, \mu - 1$$

réels (à l'exception de 0), suivant leur caractère cubique, classes

$$\begin{array}{ll} \text{A} & \alpha, \alpha', \alpha'', \dots \\ \text{B} & \beta, \beta', \beta'', \dots \\ \text{C} & \gamma, \gamma', \gamma'', \dots \end{array}$$

et en désignant par  $f$  le nombre réel qui est  $\equiv \varrho \pmod{M}$ , on

$$\alpha^{\frac{\mu-1}{3}} - 1 \equiv \beta^{\frac{\mu-1}{3}} - f \equiv \gamma^{\frac{\mu-1}{3}} - f^2 \equiv 0 \pmod{M = a + b\varrho}$$

et comme

$$\alpha^{\frac{\mu-1}{3}} - 1, \beta^{\frac{\mu-1}{3}} - f, \gamma^{\frac{\mu-1}{3}} - f^2$$

sont des nombres réels, ils doivent être divisibles non seulement par  $a + b\varrho$ , mais aussi par le module

$$p = \mu = (a + b\varrho)(a + b\varrho^2)$$

de sorte qu'on a

$$\begin{aligned} \alpha^{\frac{\mu-1}{3}} &\equiv 1 \\ \beta^{\frac{\mu-1}{3}} &\equiv f \pmod{p = \mu}. \\ \gamma^{\frac{\mu-1}{3}} &\equiv f^2 \end{aligned}$$

On voit donc que la classification des nombres

$$1, 2, 3, \dots, p-1$$

à l'aide de ces trois dernières congruences, coïncide avec celle qui a pour base leur caractère cubique par rapport au module

Le résultat

$$\left[ \frac{3}{a + b\varrho} \right] = \varrho^{-\frac{1}{3}b}$$

peut être énoncé ainsi: le nombre 3 appartient à la classe C, suivant que  $-\frac{1}{3}b$  est de la forme  $3m$ ,  $3m+1$  ou  $3m+2$ .

Voici quelques exemples.

$$p=7, \quad a=2, \quad b=3, \quad f=4.$$

$$\text{A} \quad 1, 6.$$

$$\text{B} \quad 2, 5.$$

$$\text{C} \quad 3, 4.$$

$$h \ j \ k$$

$$j \ k \ l$$

$$k \ l \ j$$

So



$p=13, a=1, b=1, f=1$	0 2 1
A 1, 5, 8, 12.	2 1 1
B 4, 6, 7, 9.	1 1 2
C 2, 3, 10, 11.	

$$p=19, a=5, b=3, f=11.$$

A 1, 7, 8, 11, 12, 18.	2 2 1
B 4, 6, 9, 10, 13, 15.	2 1 3
C 2, 3, 5, 14, 16, 17.	1 3 2

$$p=31, a=5, b=6, f=25.$$

A 1, 2, 4, 8, 15, 16, 23, 27, 29, 30.	3 4 2
B 3, 6, 7, 12, 14, 17, 19, 24, 25, 28.	4 2 4
C 5, 9, 10, 11, 13, 18, 20, 21, 22, 26.	2 4 4

$$p=37, a=-4, b=3, f=26.$$

A 1, 6, 8, 10, 11, 14, 23, 26, 27, 29, 31, 36.	2 5 4
B 2, 9, 12, 15, 16, 17, 20, 21, 22, 25, 28, 35.	5 4 3
C 3, 4, 5, 7, 13, 18, 19, 24, 30, 32, 33, 34.	4 3 5

$$p=43, a=-1, b=6, f=36.$$

A 1, 2, 4, 8, 11, 16, 21, 22, 27, 32, 35, 39, 41, 42.	3 6 4
B 3, 5, 6, 10, 12, 19, 20, 23, 24, 31, 33, 37, 38, 40.	6 4 4
C 7, 9, 13, 14, 15, 17, 18, 25, 26, 28, 29, 30, 34, 36.	4 4 6

$$p=61, a=5, b=9, f=13.$$

A 1, 3, 8, 9, 11, 20, 23, 24, 27, 28, 33, 34, 37,	6 8 5
38, 41, 50, 52, 53, 58, 60.	8 5 7
B 4, 10, 12, 14, 17, 19, 25, 26, 29, 30, 31, 32, 35,	5 7 8
36, 42, 44, 47, 49, 51, 57.	
C 2, 5, 6, 7, 13, 15, 16, 18, 21, 22, 39, 40, 43,	
45, 46, 48, 54, 55, 56, 59.	

La question de la présence du nombre 3 dans l'un des groupes A, B, C étant tranchée d'avance comme il vient d'être dit, on peut facilement, à l'aide de la loi de réciprocité dans la théorie des résidus cubiques, établir les caractères nécessaires pour reconnaître aussi la présence d'autres nombres dans ces classes. Il suffit évidemment de considérer, à ce point de vue, les nombres premiers.

En ce qui concerne le nombre premier 2, ces caractères peuvent aussi être déduits sans le secours de la loi de réciprocité, ainsi que nous allons le faire voir.

31. Le nombre  $p-1$  appartenant toujours à A, il en résulte immédiatement que 2 appartiendra à la classe A, B ou C suivant que  $\frac{p-1}{2}$  appartient à la classe A, C ou B.

Les nombres  $h, k, j$  sont respectivement les nombres de solutions des congruences

$$\begin{aligned} \alpha + \alpha' + 1 &\equiv 0 \\ \beta + \beta' + 1 &\equiv 0 \pmod{p}, \\ \gamma + \gamma' + 1 &\equiv 0 \end{aligned}$$

et comme on peut échanger entre eux  $\alpha$  et  $\alpha'$ ,  $\beta$  et  $\beta'$ ,  $\gamma$  et  $\gamma'$ , ce

trois nombres sont pairs, à l'exception du premier, lorsque  $\alpha = \alpha' = \frac{p-1}{2}$

appartient à A, ou à l'exception du second, lorsque  $\beta = \beta' = \frac{p-1}{2}$

appartient à B, ou à l'exception du troisième, lorsque  $\gamma = \gamma' = \frac{p-1}{2}$

appartient à C.

On voit donc que 2 appartient à la classe A, B ou C, suivant que les trois nombres  $h, j, k$ , le premier, le second ou le troisième est impair.

Comme on a  $p = 3n + 1$  ( $n$  pair) et, d'après le n° 28,

$$\begin{aligned} 9h &= 3n + 2a - b - 7, \\ 9j &= 3n - a + 2b - 1, \\ 9k &= 3n - a - b - 1 \end{aligned}$$

$h$  est impair lorsque  $b$  est pair,  $j$  est impair lorsque  $a$  est pair, enfin

$k$  est impair lorsque  $a$  et  $b$  sont tous les deux impairs. Puisque

$a$  et  $b$  n'ont pas de diviseur commun, aucun autre cas n'est possible

et par conséquent 2 appartient à

$$\begin{aligned} &\text{A, lorsque } b \equiv 0 \\ \text{B,} & \quad \text{,,} \quad a \equiv 0 \pmod{2}. \\ \text{C,} & \quad \text{,,} \quad a \equiv b \equiv 1 \end{aligned}$$

32. En ce qui regarde la présence de 5 dans l'une des trois classes

on a, d'après la loi de réciprocité cubique,

entiers  $a + b\varrho$ .

Pour  $a \equiv 0 \pmod{5}$ , on a donc

$$\left[\frac{5}{a + b\varrho}\right] = \left[\frac{b\varrho}{5}\right] = \left[\frac{\varrho}{5}\right] = \varrho^8 = \varrho^2;$$

et par conséquent 5 appartient à C.

Lorsque  $a$  n'est pas divisible par 5, on peut déterminer  $x$  dans

$$b \equiv ax \pmod{5},$$

et  $x$  peut prendre les valeurs 0, 1, 2, 3, 4: on a

$$\left[\frac{5}{a + b\varrho}\right] = \left[\frac{a(1 + x\varrho)}{5}\right] = \left[\frac{1 + x\varrho}{5}\right]$$

et l'on trouve ensuite

$$x=0 \quad \left[\frac{5}{a + b\varrho}\right] = 1,$$

$$x=1 \quad \left[\frac{5}{a + b\varrho}\right] = \varrho,$$

$$x=2 \quad \left[\frac{5}{a + b\varrho}\right] = 1,$$

$$x=3 \quad \left[\frac{5}{a + b\varrho}\right] = \varrho^2,$$

$$x=4 \quad \left[\frac{5}{a + b\varrho}\right] = \varrho.$$

de sorte que 5 appartient à

$$\text{A, lorsque } b \equiv 0, \quad b \equiv 2a$$

$$\text{B, } \quad \quad \quad b \equiv a, \quad b \equiv 4a \pmod{5}.$$

$$\text{C, } \quad \quad \quad b \equiv 3a, \quad a \equiv 0.$$

Pour juger de la classe de 7, on a

$$\left[\frac{7}{a + b\varrho}\right] = \left[\frac{2 + 3\varrho}{a + b\varrho}\right] \left[\frac{2 + 3\varrho^2}{a + b\varrho}\right]$$

puis, d'après la loi de réciprocité,

$$\left[\frac{7}{a + b\varrho}\right] = \left[\frac{a + b\varrho}{2 + 3\varrho}\right] \left[\frac{a + b\varrho}{2 + 3\varrho^2}\right].$$

Pour  $a \equiv 0 \pmod{7}$ , attendu qu'on a, en général,

$$\left[\frac{a + \beta\varrho}{a + b\varrho}\right] \left[\frac{a + \beta\varrho^2}{a + b\varrho^2}\right] = 1,$$

$$\left[\frac{7}{a+b\varrho}\right] = \left[\frac{\varrho}{2+3\varrho}\right] \quad \left[\frac{\varrho}{2+3\varrho^2}\right] = \left[\frac{\varrho^2}{2+3\varrho^2}\right] = \varrho^4 = \varrho,$$

de sorte que 7 appartient à B.

Lorsque  $a$  n'est pas divisible par 7, mais qu'on a

$$b \equiv ax \pmod{7},$$

il s'ensuit

$$\left[\frac{7}{a+b\varrho}\right] = \left[\frac{1+x\varrho}{2+3\varrho}\right] \quad \left[\frac{1+x\varrho}{2+3\varrho^2}\right],$$

et  $x$  peut présenter les valeurs

$$0, 1, 2, 4, 6,$$

mais non les valeurs  $x=3$  et  $x=5$ , car celles ci rendraient

$$p = a^2 - ab + b^2 \equiv a^2(1 - x + x^2)$$

divisible par 7.

On trouve maintenant

$$x=0 \quad \left[\frac{7}{a+b\varrho}\right] = 1,$$

$$x=1 \quad \left[\frac{7}{a+b\varrho}\right] = \varrho^2,$$

$$x=2 \quad \left[\frac{7}{a+b\varrho}\right] = 1,$$

$$x=4 \quad \left[\frac{7}{a+b\varrho}\right] = \varrho,$$

$$x=6 \quad \left[\frac{7}{a+b\varrho}\right] = \varrho^2,$$

de sorte que 7 appartient à

A, lorsque  $b \equiv 0$ ,  $b \equiv 2a$

B, „  $b \equiv 4a$ ,  $a \equiv 0 \pmod{7}$ .

C, „  $b \equiv a$ ,  $b \equiv 6a$

De la même manière, ou par induction, on reconnaîtra

11 appartient à

A pour  $b \equiv 0$ ,  $b \equiv 2a$ ,  $b \equiv 4a$ ,  $b \equiv 5a$

B „  $b \equiv 3a$ ,  $b \equiv 6a$ ,  $b \equiv 9a$ ,  $a \equiv 0 \pmod{11}$ ,

C „  $b \equiv a$ ,  $b \equiv 7a$ ,  $b \equiv 8a$ ,  $b \equiv 10a$

5 est aussi un nombre premier dans la théorie des nombres  
 iers  $a + b\varrho$ .

Pour  $a \equiv 0 \pmod{5}$ , on a donc

$$\left[ \frac{5}{a + b\varrho} \right] = \left[ \frac{b\varrho}{5} \right] = \left[ \frac{\varrho}{5} \right] = \varrho^3 = \varrho^2;$$

par conséquent 5 appartient à C.

Lorsque  $a$  n'est pas divisible par 5, on peut déterminer  $x$  dans

$$b \equiv ax \pmod{5},$$

peut prendre les valeurs 0, 1, 2, 3, 4: on a

$$\left[ \frac{5}{a + b\varrho} \right] = \left[ \frac{a(1 + x\varrho)}{5} \right] = \left[ \frac{1 + x\varrho}{5} \right]$$

on trouve ensuite

$$x=0 \quad \left[ \frac{5}{a + b\varrho} \right] = 1,$$

$$x=1 \quad \left[ \frac{5}{a + b\varrho} \right] = \varrho,$$

$$x=2 \quad \left[ \frac{5}{a + b\varrho} \right] = 1,$$

$$x=3 \quad \left[ \frac{5}{a + b\varrho} \right] = \varrho^2,$$

$$x=4 \quad \left[ \frac{5}{a + b\varrho} \right] = \varrho.$$

On voit que 5 appartient à

A, lorsque  $b \equiv 0, \quad b \equiv 2a$

B, "  $b \equiv a, \quad b \equiv 4a \pmod{5}.$

C, "  $b \equiv 3a, \quad a \equiv 0.$

Pour juger de la classe de 7, on a

$$\left[ \frac{7}{a + b\varrho} \right] = \left[ \frac{2 + 3\varrho}{a + b\varrho} \right] \left[ \frac{2 + 3\varrho^2}{a + b\varrho} \right]$$

d'après la loi de réciprocité,

$$\left[ \frac{7}{a + b\varrho} \right] = \left[ \frac{a + b\varrho}{2 + 3\varrho} \right] \left[ \frac{a + b\varrho}{2 + 3\varrho^2} \right].$$

$a \equiv 0 \pmod{7}$ , attendu qu'on a, en général,

$$\left[ \frac{a + \beta\varrho}{a + b\varrho} \right] \left[ \frac{a + \beta\varrho^2}{a + b\varrho^2} \right] = 1,$$

il vient

$$\left[ \frac{7}{a+b\varrho} \right] = \left[ \frac{\varrho}{2+3\varrho} \right] \quad \left[ \frac{\varrho}{2+3\varrho^2} \right] = \left[ \frac{\varrho^2}{2+3\varrho^2} \right] = \varrho^4 = \varrho,$$

de sorte que 7 appartient à B.

Lorsque  $a$  n'est pas divisible par 7, mais qu'on a

$$b \equiv ax \pmod{7},$$

il s'ensuit

$$\left[ \frac{7}{a+b\varrho} \right] = \left[ \frac{1+x\varrho}{2+3\varrho} \right] \quad \left[ \frac{1+x\varrho}{2+3\varrho^2} \right],$$

et  $x$  peut présenter les valeurs

$$0, 1, 2, 4, 6,$$

mais non les valeurs  $x=3$  et  $x=5$ , car celles ci rendraient

$$p = a^2 - ab + b^2 \equiv a^2(1 - x + x^2)$$

divisible par 7.

On trouve maintenant

$$x=0 \quad \left[ \frac{7}{a+b\varrho} \right] = 1,$$

$$x=1 \quad \left[ \frac{7}{a+b\varrho} \right] = \varrho^2,$$

$$x=2 \quad \left[ \frac{7}{a+b\varrho} \right] = 1,$$

$$x=4 \quad \left[ \frac{7}{a+b\varrho} \right] = \varrho,$$

$$x=6 \quad \left[ \frac{7}{a+b\varrho} \right] = \varrho^2,$$

de sorte que 7 appartient à

A, lorsque  $b \equiv 0$ ,  $b \equiv 2a$

B, „  $b \equiv 4a$ ,  $a \equiv 0 \pmod{7}$ .

C, „  $b \equiv a$ ,  $b \equiv 6a$

De la même manière, ou par induction, on reconnaîtra que

11 appartient à

A pour  $b \equiv 0$ ,  $b \equiv 2a$ ,  $b \equiv 4a$ ,  $b \equiv 5a$

B „  $b \equiv 3a$ ,  $b \equiv 6a$ ,  $b \equiv 9a$ ,  $a \equiv 0 \pmod{11}$ ,

C „  $b \equiv a$ ,  $b \equiv 7a$ ,  $b \equiv 8a$ ,  $b \equiv 10a$

appartient à

pour  $b = 0, b = 2a, b = 3a, b = 8a$   
 $b = a, b = 6a, b = 11a, b = 12a \pmod{13},$   
 $b = 5a, b = 7a, b = 9a, a = 0$

appartient à (mod 17),

pour  $b = 0, b = a, b = 2a, b = 9a, b = 16a, a = 0$   
 $b = 3a, b = 7a, b = 8a, b = 12a, b = 13a, b = 14a$   
 $b = 4a, b = 5a, b = 6a, b = 10a, b = 11a, b = 15a$

appartient à (mod 19),

pour  $b = 0, b = a, b = 2a, b = 10a, b = 18a, a = 0$   
 $b = 5a, b = 11a, b = 13a, b = 14a, b = 16a, b = 17a$   
 $b = 3a, b = 4a, b = 6a, b = 7a, b = 9a, b = 15a$

appartient à (mod 23),

pour  $b = 0, b = 2a, b = 5a, b = 6a, b = 7a, b = 8a, b = 11a, b = 15a$   
 $b = a, b = 9a, b = 13a, b = 16a, b = 17a, b = 18a, b = 19a, b = 22a$   
 $b = 3a, b = 4a, b = 10a, b = 12a, b = 14a, b = 20a, b = 21a, a = 0.$

La considération de ces théorèmes particuliers donne lieu aux remarques suivantes.

Pour la commodité, les nombres premiers réels de la forme  $3n-1$ , restent aussi nombres premiers dans la théorie complexe, seront désignés ici par  $Q$ , les nombres premiers de la forme  $3n+1$  par  $P$ .

Un nombre premier  $Q$  appartient, lorsque  $a \equiv 0 \pmod{Q}$ , aux classes A, B, C suivant que  $\frac{Q+1}{3}$  est de la forme  $3m, 3m+1, 3m+2$ .

Un nombre premier  $P$  appartient, lorsque  $a \equiv 0 \pmod{P}$ , aux classes A, B, C suivant que  $\frac{P-1}{3}$  est de la forme  $3m, 3m+1, 3m+2$ .

Dans les cas  $b = 0, b = 2a$ , le nombre premier  $P$  ou  $Q$  appartient toujours à la classe A.

Quand le nombre premier appartient à A pour  $a = 0$ , il appartient aussi à A pour  $b = a$  et pour  $b = -a$ . Si, au contraire, le nombre premier fait partie de la classe B ou C lorsque  $a = 0$ , il fait partie, pour  $b = a$  et  $b = -a$ , de la classe C ou B.

5. En général, les critères sont de la forme suivante:

Si  $a \equiv 0$ , le nombre premier appartient à une classe déterminée.

Si  $a$  n'est pas  $\equiv 0$ , on a  $b \equiv ax$ , et pour chaque valeur de  $x$  le nombre premier appartient à une classe déterminée, de sorte qu'on peut distribuer les valeurs de  $x$  en 3 groupes, tels que

pour  $b \equiv a\alpha$ , le nombre premier appartienne à A,

„  $b \equiv a\beta$ , „ „ „ „ B,

„  $b \equiv a\gamma$ , „ „ „ „ C.

Il faut encore ajouter le cas  $a \equiv 0$ , qui correspond aussi à une classe déterminée.

Or, le nombre total des congruences qu'on trouve de cette manière est le même pour chacune des trois classes et  $= \frac{Q+1}{3}$  ou  $= \frac{P-1}{3}$ .

6. Lorsque  $x$  et  $y$  sont deux nombres satisfaisant à la congruence

$$x + y - xy \equiv 0,$$

et que  $x$  appartient à  $\alpha$ ,  $y$  appartient également à  $\alpha$ . Mais si  $x = \beta$  ou  $x = \gamma$ ,  $y$  appartient respectivement aux  $\gamma$  ou aux  $\beta$ .

Si  $xy \equiv 1$  et que 1 appartienne aux  $\alpha$ , on a

$$\text{pour } x = \alpha' \quad y = \alpha'',$$

$$\text{„ } x = \beta' \quad y = \gamma',$$

$$\text{„ } x = \gamma' \quad y = \beta'.$$

Si  $xy \equiv 1$  et  $1 = \beta$ , on a

$$\text{pour } x = \alpha \quad y = \gamma,$$

$$\text{„ } x = \beta' \quad y = \beta'',$$

$$\text{„ } x = \gamma' \quad y = \alpha'.$$

Si  $xy \equiv 1$  et  $1 = \gamma$ , on a

$$\text{pour } x = \alpha \quad y = \beta,$$

$$\text{„ } x = \beta \quad y = \alpha,$$

$$\text{„ } x = \gamma \quad y = \gamma'.$$

34. Quant à la démonstration de ce qui vient d'être dit, la remarque 5 est la seule qui demande quelques considérations nouvelles; tout le reste n'offre, après ce qui précède, aucune difficulté.

Je vais donc prouver d'une manière générale la vérité de cette



remarque 5. Il faut pour cela distinguer les cas où le nombre premier est  $=Q$  ou  $=P$ ; commençons par le premier de ces cas, qui est de beaucoup le plus simple.

35. Lorsque le nombre premier  $Q$  est de la forme  $3n-1$ , et qu'il reste par conséquent premier aussi dans la théorie des nombres complexes de la forme  $a + b\varrho$ , on a d'après la loi de réciprocité

$$\left[ \frac{Q}{a + b\varrho} \right] = \left[ \frac{a + b\varrho}{Q} \right].$$

Soit d'abord  $a \equiv 0 \pmod{Q}$ ; dans ce cas

$$\left[ \frac{Q}{a + b\varrho} \right] = \left[ \frac{b\varrho}{Q} \right] = \left[ \frac{\varrho}{Q} \right] = \varrho^{\frac{Q-1}{3}}.$$

Mais

$$\frac{Q+1}{3} \times (Q-2)$$

est un multiple de 3 et

$$\frac{Q^3-1}{3} \equiv \frac{(Q+1)(Q-2)}{3} \equiv \frac{Q+1}{3},$$

on a par conséquent pour  $a \equiv 0 \pmod{Q}$ ,

$$\left[ \frac{Q}{a + b\varrho} \right] = \varrho^{\frac{Q+1}{3}},$$

d'où ressort l'exactitude de ce qui a été dit au n<sup>o</sup> 33 en 1.

Si  $a$  n'est pas divisible par  $Q$ ,  $x$  est complètement déterminé par

$$b \equiv ax \pmod{Q}$$

et

$$\left[ \frac{Q}{a + b\varrho} \right] = \left[ \frac{a(1+x\varrho)}{Q} \right] = \left[ \frac{1+x\varrho}{Q} \right],$$

ce qui montre déjà que la classe à laquelle appartient  $Q$  dépend uniquement de  $x$ ; pour  $x$  on peut d'ailleurs avoir évidemment les nombres

$$0, 1, 2, 3, \dots, Q-1.$$

Il ne reste plus qu'à résoudre cette question: parmi les  $Q$  quantités

$$\left[ \frac{1+x\varrho}{Q} \right] \\ (x=0, 1, 2, 3, \dots, Q-1)$$

Combien y en a-t-il d'égaux à 1, combien d'égaux à  $\varrho$ , combien d'égaux à  $\varrho^2$ ? Nous considérons un système complet de nombres non divisibles par le module, système pour lequel on peut prendre les nombres

$$\alpha + \beta \varrho$$

$$\left( \begin{matrix} \alpha \\ \beta \end{matrix} = 0, 1, 2, 3, \dots, Q-1 \right)$$

combinaison  $\alpha=0, \beta=0$  devant seule être omise. Si nous rapportons ces  $Q^2 - 1$  nombres d'après leur caractère cubique à 3 groupes A, B, C,

A	$\alpha_0 + \beta_0 \varrho, \dots$
B	$\alpha_1 + \beta_1 \varrho, \dots$
C	$\alpha_2 + \beta_2 \varrho, \dots$

Chacun de ces groupes contient

$$\frac{Q^2 - 1}{3} = (Q - 1) \times \frac{Q + 1}{3}$$

nombres, quotité qui est donc un multiple de  $Q - 1$ : et les nombres qui correspondent à  $\beta=0$ , savoir

$$1, 2, 3, \dots, Q-1,$$

appartiennent tous à A, d'où il découle que lorsque  $\alpha + \beta \varrho$  fait partie d'une certaine classe, les nombres congrus avec

$$1(\alpha + \beta \varrho), 2(\alpha + \beta \varrho), \dots, (Q-1)(\alpha + \beta \varrho)$$

font aussi partie de cette classe. Si  $\alpha$  n'est pas égal à zéro, les nombres

$$\alpha, 2\alpha, 3\alpha, \dots, (Q-1)\alpha$$

sont dans un certain ordre, sont congrus, suivant le module  $Q$ , à

$$1, 2, 3, \dots, Q-1.$$

Les nombres d'une classe, chez qui la partie réelle n'est pas zéro, peuvent donc être divisés en groupes de  $Q-1$  nombres, de telle sorte que dans chaque groupe se trouve un nombre de la forme  $\alpha + x \varrho$ .

Il ressort de là que les quotités des nombres  $1 + x\varrho$  qui rendent  $\frac{1+x\varrho}{Q}$  égal à 1,  $\varrho$  ou  $\varrho^2$ , sont

$$\frac{Q-2}{3}, \quad \frac{Q+1}{3}, \quad \frac{Q+1}{3}, \quad \text{lorsque } \left[\frac{\varrho}{Q}\right] = 1,$$

$$\frac{Q+1}{3}, \quad \frac{Q-2}{3}, \quad \frac{Q+1}{3}, \quad \text{lorsque } \left[\frac{\varrho}{Q}\right] = \varrho,$$

$$\frac{Q+1}{3}, \quad \frac{Q+1}{3}, \quad \frac{Q-2}{3}, \quad \text{lorsque } \left[\frac{\varrho}{Q}\right] = \varrho^2,$$

et comme, en outre, nous avons trouvé ci-dessus que, pour

$$a \equiv 0 \pmod{Q},$$

$a$  appartient aux classes A, B ou C suivant que  $\left[\frac{\varrho}{Q}\right]$  est égal à 1,  $\varrho$  ou  $\varrho^2$ , l'énoncé 5 du n° 33 se trouve entièrement démontré pour le cas où le nombre premier est de la forme  $3n - 1$ .

36. Lorsque le nombre premier dont on veut reconnaître la présence dans les classes A, B, C est de la forme  $P = 3n + 1$ , il s'agit de déterminer la valeur de

$$\left[\frac{P}{a + b\varrho}\right];$$

n'étant pas un nombre premier dans la théorie complexe, on doit, avant de pouvoir appliquer la loi de réciprocité, décomposer  $P$  en facteurs premiers primaires

$$P = (A + B\varrho)(A + B\varrho^2),$$

et on a alors

$$\left[\frac{P}{a + b\varrho}\right] = \left[\frac{a + b\varrho}{A + B\varrho}\right] \left[\frac{a + b\varrho}{A + B\varrho^2}\right].$$

Donc

$$\text{pour } a \equiv 0 \pmod{P}$$

$$\left[\frac{P}{a + b\varrho}\right] = \left[\frac{\varrho}{A + B\varrho}\right] \left[\frac{\varrho}{A + B\varrho^2}\right] = \varrho^{\frac{2(P-1)}{3}} = \varrho^{\frac{P-1}{6}},$$

$$\text{pour } ax \equiv b \pmod{P}$$

$$\left[\frac{P}{a + b\varrho}\right] = \left[\frac{1 + x\varrho}{A + B\varrho}\right] \left[\frac{1 + x\varrho}{A + B\varrho^2}\right].$$

Du premier résultat, pour  $a \equiv 0$ , ressort la justesse de la seconde  
marque du n° 33.

Comme  $P$  est de la forme  $3n + 1$ , la congruence

$$x^3 \equiv 1 \pmod{P}$$

a trois racines différentes,  $1, f, g$  (où  $f \equiv g^2$ ).

Les deux valeurs  $-f, -g$  ne peuvent maintenant être égales à  $x$   
s la congruence

$$b \equiv ax,$$

de  $b \equiv -af$  il résulterait

$$a^2 - ab + b^2 \equiv a^2(1 + f + f^2) \equiv 0 \pmod{P},$$

sorte que le nombre premier

$$p = a^2 - ab + b^2$$

est divisible par  $P$ .

D'après cela, les valeurs que  $x$  peut prendre sont

$$0, 1, 2, 3, \dots, P-1$$

à l'omission des nombres  $P-f$  et  $P-g$ . Leur nombre est donc  
 $P-2$ , et il s'agit de rechercher pour combien de ces  $P-2$  valeurs  
 $x$  l'expression

$$\left[ \frac{1+x\varrho}{A+B\varrho} \right] \left[ \frac{1+x\varrho}{A+B\varrho^2} \right]$$

prend les valeurs  $1, \varrho$  et  $\varrho^2$ .

Je fais remarquer encore que

$$\left[ \frac{\varrho}{A+B\varrho} \right] = \varrho^{\frac{P-1}{3}}$$

car, pour  $a \equiv 0 \pmod{P}$  on avait

$$\left[ \frac{P}{a+b\varrho} \right] = \varrho^{\frac{2(P-1)}{3}}.$$

Ainsi, lorsque  $\varrho$ , pour le module  $A+B\varrho$ , appartient à la classe  
 $B$  ou  $C$ , il arrive simultanément que  $P$ , pour le module  $a+b\varrho$   
, ce qui est la même chose, pour le module réel  $p$ ), appartient  
à la classe  $A, C$  ou  $B$ .

7. Un nombre arbitraire  $a + \beta\varrho$  étant donné, on peut toujours  
trouver un autre nombre qui lui soit congru suivant le module  
 $A+B\varrho$  et dont la partie réelle soit 1.

La division d'un système complet de nombres non divisibles par module, en trois classes, d'après leur caractère cubique, peut donc être représentée de cette manière

$$(\text{mod } A + B \varrho)$$

A	$\alpha = 1 + a \varrho,$	$\alpha' = 1 + a' \varrho,$	$\alpha'' = 1 + a'' \varrho, \dots$
B	$\beta = 1 + b \varrho,$	$\beta' = 1 + b' \varrho,$	$\beta'' = 1 + b'' \varrho, \dots$
C	$\gamma = 1 + c \varrho,$	$\gamma' = 1 + c' \varrho,$	$\gamma'' = 1 + c'' \varrho, \dots$

comme, de

$$(1 + a \varrho)^{\frac{P-1}{3}} - \varrho^k \equiv (A + B \varrho) (C + D \varrho)$$

suit

$$(1 + a \varrho^2)^{\frac{P-1}{3}} - \varrho^{2k} \equiv (A + B \varrho^2) (C + D \varrho^2),$$

classification pour le module  $A + B \varrho^2$  peut simultanément être présentée par

$$(\text{mod } A + B \varrho^2)$$

A	$1 + a \varrho^2,$	$1 + a' \varrho^2,$	$1 + a'' \varrho^2, \dots$
B	$1 + c \varrho^2,$	$1 + c' \varrho^2,$	$1 + c'' \varrho^2, \dots$
C	$1 + b \varrho^2,$	$1 + b' \varrho^2,$	$1 + b'' \varrho^2, \dots$

Les nombres  $a, b, c, a', b', c', a'', b'', c'', \dots$  forment, dans leur ensemble, tous les nombres du groupe

$$0, 1, 2, 3, \dots, P-1,$$

l'exception du seul nombre qui est  $\equiv -\varrho^2 \pmod{A + B \varrho}$  et qui est congru suivant le module  $P$  à un des nombres  $-f, -g$ . Les cas où l'on a

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = 1$$

ont évidemment

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = 1 \text{ et simultanément } \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = 1,$$

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = \varrho \text{ et simultanément } \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = \varrho^2,$$

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] = \varrho^2 \text{ et simultanément } \left[ \frac{1 + x \varrho}{A + B \varrho^2} \right] = \varrho.$$

Or,  $\left[\frac{1+x\varrho}{A+B\varrho}\right]$  est égal à 1 pour  $x=a, a', a'', \dots$ , et pour qu'on ait en même temps  $\left[\frac{1+x\varrho}{A+B\varrho^2}\right]=1$ , il faut donc que  $1+a\varrho$  soit congru suivant le module  $A+B\varrho^2$  à un des nombres  $1+a\varrho^2, 1+a'\varrho^2, \dots$ , c'est-à-dire

$$1+a\varrho \equiv 1+a'\varrho^2 \pmod{A+B\varrho^2};$$

reciproquement, s'il est satisfait à cette congruence, on a

$$\left[\frac{1+a\varrho}{A+B\varrho}\right]=1, \quad \left[\frac{1+a\varrho}{A+B\varrho^2}\right]=1.$$

Le nombre des fois où ce cas se présente est donc égal au nombre des solutions de la congruence ci-dessus. En raisonnant d'une manière analogue pour les deux autres cas

$$\left[\frac{1+x\varrho}{A+B\varrho}\right]=\varrho, \quad \left[\frac{1+x\varrho}{A+B\varrho^2}\right]=\varrho^2$$

$$\left[\frac{1+x\varrho}{A+B\varrho}\right]=\varrho^2, \quad \left[\frac{1+x\varrho}{A+B\varrho^2}\right]=\varrho,$$

on trouve que le nombre des fois où

$$\left[\frac{1+x\varrho}{A+B\varrho}\right] \left[\frac{1+x\varrho}{A+B\varrho^2}\right]$$

devient égal à 1, est représenté par la somme des nombres de solutions des trois congruences

$$\begin{aligned} 1+a\varrho &\equiv 1+a'\varrho^2 \\ 1+b\varrho &\equiv 1+b'\varrho^2 \pmod{A+B\varrho^2}. \\ 1+c\varrho &\equiv 1+c'\varrho^2 \end{aligned}$$

On reconnaîtra, de même, que le nombre des fois où l'expression précédente devient égal à  $\varrho$  et à  $\varrho^2$  est exprimé, dans le premier cas, par la somme des nombres de solutions des congruences

$$\begin{aligned} 1+b\varrho &\equiv 1+a\varrho^2 \\ 1+c\varrho &\equiv 1+b\varrho^2 \pmod{A+B\varrho^2}, \\ 1+a\varrho &\equiv 1+c\varrho^2 \end{aligned}$$

et, dans le second cas, par la somme des nombres de solutions des congruences

$$\begin{aligned} 1 + c \varrho &\equiv 1 + a \varrho^2 \\ 1 + a \varrho &\equiv 1 + b \varrho^2 \pmod{A + B \varrho^2}. \\ 1 + b \varrho &\equiv 1 + c \varrho^2 \end{aligned}$$

Pour pouvoir appliquer directement les développements des nos 25—28, il est un peu plus facile de considérer seulement des congruences suivant le module  $A + B \varrho$ , de sorte que, remplaçant partout dans les formules précédentes  $\varrho$  par  $\varrho^2$  et désignant par  $t, u, v$  les nombres de fois que

$$\left[ \frac{1 + x \varrho}{A + B \varrho} \right] \times \left[ \frac{1 + x \varrho^2}{A + B \varrho^2} \right]$$

est respectivement égal à 1,  $\varrho$  ou  $\varrho^2$ , nous écrivons :

$t$  = somme des nombres de solutions de

$$\begin{aligned} 1 + a \varrho^2 &\equiv 1 + a' \varrho \\ 1 + b \varrho^2 &\equiv 1 + b' \varrho \pmod{A + B \varrho}, \\ 1 + c \varrho^2 &\equiv 1 + c' \varrho \end{aligned}$$

$u$  = somme des nombres de solutions de

$$\begin{aligned} 1 + b \varrho^2 &\equiv 1 + a \varrho \\ 1 + c \varrho^2 &\equiv 1 + b \varrho \pmod{A + B \varrho}, \\ 1 + a \varrho^2 &\equiv 1 + c \varrho \end{aligned}$$

$v$  = somme des nombres de solutions de

$$\begin{aligned} 1 + c \varrho^2 &\equiv 1 + a \varrho \\ 1 + a \varrho^2 &\equiv 1 + b \varrho \pmod{A + B \varrho}. \\ 1 + b \varrho^2 &\equiv 1 + c \varrho \end{aligned}$$

38. A ce sujet, il convient encore de remarquer ce qui suit. Parmi les nombres  $a, b, c, a', b', c'$  ne se trouve pas l'un des deux nombres  $-f, -g$ . Supposons que ce soit  $-f$ , de sorte que  $-g$  s'y trouve. Il n'en est alors pas moins évident que cette valeur  $-g$  ne peut se présenter nulle part dans l'une des congruences ci-dessus; car, de  $1 + a \varrho^2 \equiv 1 + a' \varrho$  ou  $a \varrho^2 = a' \varrho$  par exemple, il suivrait, pour  $a = -g, a' \equiv a \varrho \equiv -\varrho^2 \equiv -f$  (puisque  $f = \varrho^2$  et  $g = \varrho \pmod{A + B \varrho}$ ); or, la valeur  $a' \equiv -f$  ne se présente pas. Comme, parmi les valeurs à prendre pour  $x$ , ne se trouvaient ni  $-f$  ni  $-g$ ,

en ressort avec évidence que les expressions ci-dessus données pour  $t$ ,  $u$  et  $v$  sont réellement exactes, lorsque les nombres  $a$ ,  $a'$ ,  $b$ ,  $b'$ ,  $c$ ,  $c'$  qui entrent, dans les congruences, sont choisis de toutes les manières possibles dans les groupes  $a, a', a'', \dots, b, b', b'', \dots, c, c', c'', \dots$ . En introduisant, au lieu de  $a, b, \dots$  les nombres  $a \equiv 1 + a\varrho$ ,  $b \equiv 1 + b\varrho$ , on trouve, par exemple, que  $a\varrho^2 \equiv a'\varrho$  se transforme en

$$\varrho(a-1) \equiv a' - 1,$$

$$a' - \varrho a \equiv 1 - \varrho,$$

en agissant de même avec les autres congruences, on obtient les expressions suivantes

= somme des nombres de solutions de

$$\begin{aligned} a' - \varrho a &\equiv 1 - \varrho \\ \beta' - \varrho \beta &\equiv 1 - \varrho \pmod{A + B\varrho}, \\ \gamma' - \varrho \gamma &\equiv 1 - \varrho \end{aligned}$$

= somme des nombres de solutions de

$$\begin{aligned} a - \varrho \beta &\equiv 1 - \varrho \\ \beta - \varrho \gamma &\equiv 1 - \varrho \pmod{A + B\varrho}, \\ \gamma - \varrho a &\equiv 1 - \varrho \end{aligned}$$

= somme des nombres de solutions de

$$\begin{aligned} a - \varrho \gamma &\equiv 1 - \varrho \\ \beta - \varrho a &\equiv 1 - \varrho \pmod{A + B\varrho}, \\ \gamma - \varrho \beta &\equiv 1 - \varrho \end{aligned}$$

Dans le premier membre de ces congruences le signe  $-$  peut tout être remplacé par  $+$ , puisque deux nombres  $\lambda$  et  $-\lambda$  appartiennent toujours à la même classe. Ce remplacement étant effectué, toutes les congruences étant en outre multipliées par le nombre tiers,

$$\frac{P-1}{1-\varrho} = \frac{3n}{1-\varrho} = n(1-\varrho^2),$$

vient:

= somme des nombres de solutions de

$$\begin{aligned} a' + \varrho a + 1 &\equiv 0 \\ \beta' + \varrho \beta + 1 &\equiv 0 \pmod{A + B\varrho}, \\ \gamma' + \varrho \gamma + 1 &\equiv 0 \end{aligned}$$



$u$  = somme des nombres de solutions de

$$\begin{aligned} \alpha + \varrho \beta + 1 &\equiv 0 \\ \beta + \varrho \gamma + 1 &\equiv 0 \pmod{A + B\varrho}, \\ \gamma + \varrho \alpha + 1 &\equiv 0 \end{aligned}$$

$v$  = somme des nombres de solutions de

$$\begin{aligned} \alpha + \varrho \gamma + 1 &\equiv 0 \\ \beta + \varrho \alpha + 1 &\equiv 0 \pmod{A + B\varrho}, \\ \gamma + \varrho \beta + 1 &\equiv 0 \end{aligned}$$

On arrive à ce résultat dans chacune des trois suppositions qui peuvent être faites, à savoir, que  $n(1 - \varrho^2)$  fait partie de la classe A, B ou C. Cela tient évidemment à ce que les groupes de 3 congruences, qui viennent d'être trouvés, sont tels qu'ils n'éprouvent aucun changement par une permutation cyclique de  $\alpha, \beta, \gamma$ .

Il y a maintenant trois cas à distinguer:

I.  $\varrho$  appartenant à A, ou  $\left[ \frac{\varrho}{A + B\varrho} \right] = 1$ .

Dans ce cas, on a  $\varrho \alpha = \alpha'', \varrho \beta = \beta'', \varrho \gamma = \gamma''$ , et par conséquent  $t, u, v$  sont les sommes des nombres de solutions des congruences suivantes

$t$		$u$		$v$
$\alpha + \alpha' + 1 \equiv 0,$		$\alpha + \beta + 1 \equiv 0,$		$\alpha + \gamma + 1 \equiv 0,$
$\beta + \beta' + 1 \equiv 0,$		$\beta + \gamma + 1 \equiv 0,$		$\beta + \alpha + 1 \equiv 0,$
$\gamma + \gamma' + 1 \equiv 0,$		$\gamma + \alpha + 1 \equiv 0,$		$\gamma + \beta + 1 \equiv 0,$

ou, d'après le n° 25, si les résultats trouvés à cet endroit pour le nombre premier  $a + b\varrho$  sont transportés au module  $A + B\varrho$  avec la norme  $3n + 1$ ,

$$\begin{aligned} t &= h + k + j = n - 1, \\ u &= j + l + k = n, \\ v &= k + j + l = n. \end{aligned}$$

D'après le n° 36, on a dans ce cas, pour  $a \equiv 0$ ,  $\left[ \frac{P}{a + b\varrho} \right] = 1$ .

II.  $\varrho$  appartient à B, ou  $\left[ \frac{\varrho}{A + B\varrho} \right] = \varrho$ .

$t, u, v$  sont alors les sommes des nombres de solutions des congruences suivantes

$$\begin{array}{c|c|c} t & u & v \\ \hline \alpha + \beta + 1 \equiv 0, & \alpha + \gamma + 1 \equiv 0, & \alpha + \alpha' + 1 \equiv 0, \\ \beta + \gamma + 1 \equiv 0, & \beta + \alpha + 1 \equiv 0, & \beta + \beta' + 1 \equiv 0, \\ \gamma + \alpha + 1 \equiv 0, & \gamma + \beta + 1 \equiv 0, & \gamma + \gamma' + 1 \equiv 0, \end{array}$$

bien

$$\begin{aligned} t &= n, \\ u &= n, \\ v &= n - 1. \end{aligned}$$

D'après le n° 36, on a dans ce cas, pour  $\alpha \equiv 0$ ,  $\left[ \frac{P}{a + b\varrho} \right] = \varrho^2$ .

III.  $\varrho$  appartient à C, ou  $\left[ \frac{\varrho}{A + B\varrho} \right] = \varrho^2$ .

$u, v$  sont alors les sommes des nombres de solutions de

$$\begin{array}{c|c|c} t & u & v \\ \hline \alpha + \gamma + 1 \equiv 0, & \alpha + \alpha' + 1 \equiv 0, & \alpha + \beta + 1 \equiv 0, \\ \beta + \alpha + 1 \equiv 0, & \beta + \beta' + 1 \equiv 0, & \beta + \gamma + 1 \equiv 0, \\ \gamma + \beta + 1 \equiv 0, & \gamma + \gamma' + 1 \equiv 0, & \gamma + \alpha + 1 \equiv 0, \end{array}$$

bien

$$\begin{aligned} t &= n, \\ u &= n - 1, \\ v &= n. \end{aligned}$$

D'après le n° 36, on a dans ce cas, pour  $\alpha \equiv 0$ ,  $\left[ \frac{P}{a + b\varrho} \right] = \varrho$ .

Par là se trouve démontré tout ce qui a été dit au n° 33 concernant la forme générale des caractères qui permettent de reconnaître à laquelle des trois classes appartient un nombre premier donné.

39. Quant aux autres énoncés du n° 33, il suffira de remarquer que ce qui a été dit en 6 résulte immédiatement des formules

$$\begin{aligned} \left[ \frac{1 + x\varrho}{Q} \right] \left[ \frac{1 + y\varrho}{Q} \right] &= \left[ \frac{1 - xy + (x + y - xy)\varrho}{Q} \right] \\ \left[ \frac{x\varrho}{A + B\varrho} \right] \left[ \frac{1 + x\varrho}{A + B\varrho^2} \right] \left[ \frac{1 + y\varrho}{A + B\varrho} \right] \left[ \frac{1 + y\varrho}{A + B\varrho^2} \right] &= \\ &= \left[ \frac{1 - xy + (x + y - xy)\varrho}{A + B\varrho} \right] \left[ \frac{1 - xy + (x + y - xy)\varrho}{A + B\varrho^2} \right]. \end{aligned}$$

de la remarque, que pour  $b = 2a$  le nombre premier (2, 5, 7, 11, ...) appartient toujours à la classe A, on peut encore déduire une conséquence qu'il paraît utile de noter ici. Puisque, à cause de

$$4p = 4(a^2 - ab + b^2) = (2a - b)^2 + 3b^2$$

$a$  fait pas partie des facteurs premiers de  $2a - b$ , il s'ensuit que les facteurs premiers de  $2a - b$  sont des résidus cubiques de  $p$ , par conséquent  $2a - b$  lui-même est résidu cubique de  $p$ .

A ce même résultat conduit aussi la considération suivante, tout autre nature.

Soit  $p = 3n + 1$  et supposons que  $z$  parcoure un système complet de nombres incongrus, non divisibles par le module  $a + be$ ; de l'équation

$$(z^n + 1)^{2n} = z^{2n} + \dots + \frac{2n(2n-1)\dots(n+1)}{1 \cdot 2 \cdot 3 \dots n} z^n + \dots + 1$$

il s'ensuit alors

$$\Sigma (z^n + 1)^{2n} \equiv 2 \dots \frac{2n(2n-1)\dots(n+1)}{1 \cdot 2 \cdot 3 \dots n} \pmod{a + be}.$$

Mais, d'un autre côté, les nombres  $z^1, \dots$  forment tous des résidus cubiques de  $a + be$ , chaque résidu étant écrit 3 fois, et parmi les termes  $z^n + 1$  il y en a donc  $3h$  qui appartiennent à la classe A,  $3k$  à B,  $3l$  à C; par conséquent, on a aussi

$$\Sigma (z^n + 1)^{2n} \equiv 3h + 3ke + 3le \pmod{a + be},$$

d'après les valeurs du n° 28,

$$\Sigma (z^n + 1)^{2n} \equiv a - b - 2 - be.$$

On en résulte

$$\frac{2n(2n-1)\dots(n+1)}{1 \cdot 2 \cdot 3 \dots n} \equiv a - b - be - 2a - b \pmod{a + be},$$

ce qu'on a aussi

$$2a - b \equiv \frac{2n(2n-1)\dots(n+1)}{1 \cdot 2 \cdot 3 \dots n} \pmod{p = 3n + 1}$$

une conséquence remarquable, donnée pour la première fois par Jacobi, dans le Journal de Crelle, t. 2, et dont la démonstration est ordinairement déduite de formules employées dans la théorie de la division du cercle.

En écrivant cette congruence sous la forme

$$(1 \cdot 2 \cdot 3 \cdot \dots \cdot n)^2 (2a - b) \equiv -1 \cdot 2 \cdot 3 \cdot \dots \cdot (2n) \pmod{p},$$

et en observant que

$$2n + 1 \equiv -n,$$

$$2n + 2 \equiv -(n - 1),$$

$$2n + 3 \equiv -(n - 2),$$

• • • • •

$$3n \equiv -1,$$

que  $n$  est pair et  $1. 2. 3. \dots (3n) \equiv -1$ , on obtient

$$(1. 2. 3. \dots n)^3 (2a - b) \equiv 1 \pmod{p},$$

d'où il ressort immédiatement que  $2a - b$  est résidu cubique de  $p$ , ainsi que nous l'avions déjà trouvé ci-dessus, par une voie toute différente. Cette première démonstration nous avait appris, en outre, que tous les diviseurs de  $2a - b$  sont des résidus cubiques.

# XI.

(Paris, C.-R. Acad. Sci., 95, 1882, 901—903).

## Sur un théorème de M. Tisserand.

(Extrait d'une lettre adressée à M. Hermite.)

Soit

$$T = [(x_1 - c_1)^2 + (x_2 - c_2)^2 + (x_3 - c_3)^2 + (x_4 - c_4)^2]^{-1};$$

rs

$$\dots \dots \dots \frac{\partial^2 T}{\partial x_1^2} + \frac{\partial^2 T}{\partial x_2^2} + \frac{\partial^2 T}{\partial x_3^2} + \frac{\partial^2 T}{\partial x_4^2} = 0.$$

Posons

$$\begin{aligned} x_1 &= r \cos u \cos x, & c_1 &= a \cos u' \cos x', \\ x_2 &= r \cos u \sin x, & c_2 &= a \cos u' \sin x', \\ x_3 &= r \sin u \cos y, & c_3 &= a \sin u' \cos y', \\ x_4 &= r \sin u \sin y, & c_4 &= a \sin u' \sin y'; \end{aligned}$$

aura

$$T = (a^2 - 2ar \cos \varphi + r^2)^{-1},$$

$$\dots \cos \varphi = \cos u \cos u' \cos (x - x') + \sin u \sin u' \cos (y - y'),$$

par l'introduction des variables  $r, u, x, y$ , l'équation (1) se transforme ainsi

$$\dots \dots \dots \begin{cases} \frac{\partial}{\partial r} \left( r^3 \sin u \cos u \frac{\partial T}{\partial r} \right) + \frac{\partial}{\partial u} \left( r \sin u \cos u \frac{\partial T}{\partial u} \right) \\ + \frac{\partial}{\partial x} \left( r \tan u \frac{\partial T}{\partial x} \right) + \frac{\partial}{\partial y} \left( r \cot u \frac{\partial T}{\partial y} \right) = 0. \end{cases}$$

En développant  $T$  suivant les puissances ascendantes de  $r$ , on a

$$T = \sum_0^{\infty} \frac{r^n}{a^{n+2}} \frac{\sin (n+1) \varphi}{\sin \varphi} = \sum_0^{\infty} \frac{V^{(n)} r^n}{a^{n+2}},$$

et, substituant cette valeur dans (3), on obtient l'équation différentielle suivante pour  $V^{(n)} = \frac{\sin(n+1)\varphi}{\sin\varphi}$  considérée comme fonction de  $u, x, y$  par la substitution (2)

$$(4) \quad \frac{\partial^2 V^{(n)}}{\partial u^2} + \frac{1}{\cos^2 u} \frac{\partial^2 V^{(n)}}{\partial x^2} + \frac{1}{\sin^2 u} \frac{\partial^2 V^{(n)}}{\partial y^2} + 2 \cot 2u \frac{\partial V^{(n)}}{\partial u} + n(n+2)V^{(n)} = 0;$$

$V^{(n)}$  est une fonction entière du degré  $n$  de  $\cos\varphi$ , et l'on aura donc

$$(5) \quad \begin{cases} V^{(n)} = R_{0,0}^{(n)} + 2 \Sigma R_{i,0}^{(n)} \cos i(x-x') \\ \quad + 2 \Sigma R_{0,k}^{(n)} \cos k(y-y') + 4 \Sigma \Sigma R_{i,k}^{(n)} \cos i(x-x') \cos k(y-y'). \end{cases}$$

Il est évident que l'on n'a qu'à considérer les  $R_{i,k}^{(n)}$  où  $n+i+k$  est pair. Les  $R_{i,k}^{(n)}$  sont des fonctions entières de  $\cos u \cos u'$  et  $\sin u \sin u'$ , et l'on voit facilement que  $R_{i,k}^{(n)}$  doit contenir le facteur  $(\cos u \cos u')^i (\sin u \sin u')^k$ .

Maintenant, à l'aide de (4), on obtient

$$(6) \quad \frac{d^2 R_{i,k}^{(n)}}{du^2} + 2 \cot 2u \frac{dR_{i,k}^{(n)}}{du} + \left[ n(n+2) - \frac{i^2}{\cos^2 u} - \frac{k^2}{\sin^2 u} \right] R_{i,k}^{(n)} = 0.$$

En posant

$$R_{i,k}^{(n)} = \cos^i u \sin^k u S_{i,k}^{(n)},$$

$$t = \sin^2 u,$$

l'équation (6) devient

$$t(1-t) \frac{d^2 S_{i,k}^{(n)}}{dt^2} + [\gamma - (\alpha + \beta + 1)t] \frac{dS_{i,k}^{(n)}}{dt} - \alpha \beta S_{i,k}^{(n)} = 0,$$

où

$$\alpha = \frac{i+k-n}{2},$$

$$\beta = \frac{i+k+n+2}{2},$$

$$\gamma = k+1.$$

C'est l'équation de la série hypergéométrique; donc

$$S_{i,k}^{(n)} = {}_2F_1(\alpha, \beta, \gamma, \sin^2 u),$$

${}_2F_1$  étant indépendant de  $u$ . On voit que  $S_{i,k}^{(n)}$  est une fonction entière de  $\sin^2 u$ ,  $\alpha$  étant un nombre entier négatif.

en conclut facilement la valeur suivante de  $R_{l,k}^{(m)}$ :

$$R_{l,k}^{(m)} = c_{l,k}^{(m)} (\cos u \cos u')^l (\sin u \sin u')^k \mathcal{F}(\alpha, \beta, \gamma, \sin u) \\ \times \mathcal{F}(\alpha, \beta, \gamma, \sin u'),$$

est une constante numérique.

On obtiens la valeur de  $c_{l,k}^{(m)}$  en posant  $u = u'$ ,  $\sin u = 1$ .

On compare alors, dans l'équation (5), les termes avec  $l^n$ , on vient au développement

$$(\cos y - \cos x)^n = \sum \sum c_{l,k}^{(n)} \cos l x \cos k y,$$

est facile d'obtenir d'une manière directe en exprimant les  $c_{l,k}^{(n)}$  en intégrales définies.

On pose  $u = u' = \frac{1}{2} \pi$ ,  $x' = 0$ ,  $y' = 0$  dans les équations (5) et (7), on tombe sur la formule spéciale obtenue pour la première fois par L. Tisserand (Comptes rendus, t. 88 et 89)

## XII.

(Paris, C.-R. Acad. Sci., 95, 1882, 1043—1044.)

### Sur un théorème de M. Tisserand.

(Note présentée par M. Hermite.)

J'ai été conduit à la généralisation suivante de la formule donnée dans ma communication précédente.

Posons

$$P^{(n)}(p, x) = 2^n \frac{\Pi\left(n + \frac{p-3}{2}\right)}{\Pi(n)} \left[ x^n - \frac{n(n-1)}{2(2n+p-3)} x^{n-2} + \frac{n(n-1)(n-2)(n-3)}{2 \cdot 4 \cdot (2n+p-3)(2n+p-5)} x^{n-4} - \dots \right],$$

étant un nombre entier, non négatif,  $p$  un nombre quelconque.

On a, en particulier,

$$P^{(n)}(1, x) = \frac{2}{n} \cos nu, \quad x = \cos u,$$

$$P^{(n)}(2, x) = \sqrt{\pi} X_n,$$

$$P^{(n)}(3, x) = \frac{\sin(n+1)u}{\sin u}.$$

Je remarque que, en accord avec la définition (1), on doit prendre, dans les formules suivantes

$$nP^{(n)}(1, x) = 1 \quad \text{pour } n = 0.$$

Ces polynômes ont été étudiés, sous le nom de fonctions sphériques d'ordre  $p$ , par M. Heine, et l'on a

$$\frac{\Pi\left(\frac{p-3}{2}\right)}{(1-2ax+a^2)^{\frac{p-1}{2}}} = \sum_0^{\infty} a^n P^{(n)}(p, x),$$

$$-\log(1-2ax+a^2) = \sum_1^{\infty} a^n P^{(n)}(1, x).$$



aisons maintenant

$$X = x \cos u \cos u' + y \sin u \sin u';$$

je dis qu'on aura

$$\begin{aligned} P^{(n)}(p, X) &= \sum \sum c_{i,k} (\cos u \cos u')^i (\sin u \sin u')^k \\ &\times \mathfrak{F}\left(\begin{matrix} i+k-n \\ 2 \end{matrix}, \begin{matrix} i+k+n+p-1 \\ 2 \end{matrix}, \begin{matrix} k+\frac{p+1}{4} \\ 4 \end{matrix}, \sin^2 u\right) \\ &\times \mathfrak{F}\left(\begin{matrix} i+k-n \\ 2 \end{matrix}, \begin{matrix} i+k+n+p-1 \\ 2 \end{matrix}, \begin{matrix} k+\frac{p+1}{4} \\ 4 \end{matrix}, \sin^2 u'\right) \\ &\times P^{(n)}\left(\frac{p-1}{2}, x\right) P^{(n)}\left(\frac{p-1}{2}, y\right) \end{aligned}$$

la sommation s'étend à toutes les valeurs entières non négatives  
et de  $k$ , qui rendent  $n-i-k$  pair et non négatif  
la valeur de la constante numérique  $c_{i,k}$  est la suivante

$$\begin{aligned} c_{i,k} &= \left(i + \frac{p-3}{4}\right) \left(k + \frac{p-3}{4}\right) \\ &\quad \Pi\left(\begin{matrix} n-i+k+\frac{p-3}{4} \\ 2 \end{matrix}\right) \Pi\left(\begin{matrix} n+i+k+p-3 \\ 2 \end{matrix}\right) \\ &\times \Pi\left(\begin{matrix} n-i-k \\ 2 \end{matrix}\right) \Pi\left(k + \frac{p-3}{4}\right) \Pi\left(k + \frac{p-3}{4}\right) \Pi\left(\begin{matrix} n+i-k+\frac{p-3}{4} \\ 2 \end{matrix}\right) \end{aligned}$$

pour  $p=3$ ,  $u=u'$ , on retrouve la formule de M. Tissierand.

l'on pose  $u=u'=0$ , tous les termes dans lesquels  $k$  n'est pas  
à zéro disparaissent, et l'on obtient le développement de  $P^{(n)}(p, x)$

ant les polynômes  $P^{(n)}\left(\frac{p-1}{2}, x\right)$ .

### XIII.

Amsterdam, Nieuw Arch. Wisk., 9, 1882, 196—197.)

---

s van de stelling, dat eene geheele rationale functie  
 tijd, voor zekere reële of complexe waarden van  
 de veranderlijke, de waarde nul aanneemt.

Volgende bewijs van dit fundamenteel-theorema der stelskunde,  
 na zooverre de hulpmiddelen der integraalrekening te hulp  
 worden, eenige verwantschap met het derde bewijs van  
 Werke, III, p. 59). De wijze echter, waarop de tegenspraak  
 wordt uit de onderstelling, dat de stelling niet waar was,  
 geheel anders.

$f(z) = z^n + az^{n-1} + bz^{n-2} + \dots$  eene geheele rationale functie  
 $n^{\text{den}}$  graad, en voor  $z = x + yi$

$$f(z) = u + vi.$$

functies  $u$  en  $v$ , die geheel rationaal in  $x$  en  $y$  zijn, hebben  
 voor het volgende wezenlijke eigenschap, dat hoe groot een  
 ook gegeven is, men altijd een getal  $R$  zóó groot kan be-  
 at voor alle waarden van  $x$  en  $y$ , die aan de voorwaarde

$$x^2 + y^2 \geq R^2$$

$u^2 + v^2$  grooter dan  $A$  is.

s niet noodig bij het bewijs van deze bekende eigenschap  
 staan; en ik merk hier alleen op, dat zij ten slotte daarop  
 dat de „norm” van het product van twee complexe getallen  
 aan het product der normen van de factoren, en dat dus

$$(x + yi)^n = p + qi$$

, tegelijkertijd identiek

$$(x^2 + y^2)^n = p^2 + q^2$$

Bewezen moet worden, dat er (reële) waarden van  $x$  en  $y$  zijn, die gelijktijdig  $u=0$  en  $v=0$  maken

Inderdaad, bestonden er zulke waarden niet, dan zoude

$$w = \log(u^2 + v^2)$$

ne functie van  $x$  en  $y$  zijn, die de volgende eigenschappen had.

Ten eerste,  $w$  zou voor alle waarden van  $x$  en  $y$  eindig en continu zijn, en gedeeltelijke afgeleiden naar  $x$  en  $y$  hebben van alle waarden, die evenzeer eindig en continu zijn voor alle waarden van  $x$  en  $y$ .

Ten tweede, de functie  $w$  voldoet aan de vergelijking

$$\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} = 0.$$

Dit laatste is duidelijk, wanneer men bedenkt, dat  $\frac{1}{2} \log(u^2 + v^2)$  het reële deel is van de functie  $\log f(z)$  van de complexe veranderlijke  $z$ . Maar men kan het ook direct toelichten, wanneer men bedenkt, dat

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}$$

. Men heeft namelijk

$$\frac{\partial w}{\partial x} = 2 \frac{u \frac{\partial u}{\partial x} + v \frac{\partial v}{\partial x}}{u^2 + v^2} = 2 \frac{u \frac{\partial v}{\partial y} - v \frac{\partial u}{\partial y}}{u^2 + v^2} = 2 \frac{\partial}{\partial y} \left( \arctg \frac{v}{u} \right),$$

$$\frac{\partial w}{\partial y} = 2 \frac{u \frac{\partial u}{\partial y} + v \frac{\partial v}{\partial y}}{u^2 + v^2} = 2 \frac{-u \frac{\partial v}{\partial x} + v \frac{\partial u}{\partial x}}{u^2 + v^2} = -2 \frac{\partial}{\partial x} \left( \arctg \frac{v}{u} \right),$$

is

$$\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} = 0.$$

Maar voor de functien, die de eigenschappen hebben, waaraan  $w$  voldoet, geldt een theorema dat, — wanneer men de veranderlijken  $x$  en  $y$  meerkundig voorstelt, door de punten in een vlak, waarbij de veranderlijken  $x$  en  $y$  rechthoekige coördinaten zijn, — waarin bestaat, dat de waarde van de functie in een willekeurig

unt even groot is als het gemiddelde der waarden, die de functie aanneemt op den omtrek van een cirkel, waarvan dat punt het middelpunt is. Dus scherper in eene analytische formule uitgedrukt

$$w(x_0, y_0) = \frac{1}{2\pi} \int_0^{2\pi} w(x_0 + R \cos \varphi, y_0 + R \sin \varphi) d\varphi.$$

Zie bijv. Rieman's Inaug. Diss. Art. 10, Gesamm. Werke, p. 20.) Maar dit voert hier blijkbaar tot eene ongerijmdheid, want men kan altijd zoo groot aannemen, dat

$$w(x_0 + R \cos \varphi, y_0 + R \sin \varphi) = \log(u^2 + v^2)$$

voor alle waarden van  $\varphi$ , grooter is dan een geheel willekeurig aangenomen getal.

De onderstelling, dat er geene waarden van  $x$  en  $y$  zijn, die tegelijkertijd  $u=0$  en  $v=0$  maken, moet dus valsch zijn.

---

### XIII.

(Amsterdam, Nieuw Arch. Wisk., 9, 1882, 196—197.)

(traduction)

---

**Preuve du théorème, d'après lequel une fonction entière et rationnelle s'annule pour certaines valeurs réelles ou complexes de la variable.**

La preuve suivante de ce théorème fondamental de l'algèbre possède quelque analogie avec la troisième démonstration de Gauss (Werke, II, p. 59); en effet, nous nous servons également du calcul intégral. Mais la façon dont la contradiction est déduite de l'hypothèse que le théorème est faux est tout autre dans cet article.

Soit  $f(z) = z^n + az^{n-1} + bz^{n-2} + \dots$  une fonction entière et rationnelle du degré  $n$ , et supposons que pour  $z = x + yi$  on ait

$$f(z) = u + vi.$$

Les fonctions  $u$  et  $v$  entières et rationnelles en  $x$  et  $y$  possèdent alors cette propriété qui nous sera nécessaire dans la suite que, quelque grand que soit un nombre donné  $A$ , on peut toujours déterminer un nombre  $R$  de grandeur telle que pour toutes les valeurs de  $x$  et de  $y$  qui satisfont à la condition

$$x^2 + y^2 \geq R^2,$$

l'expression  $u^2 + v^2$  est supérieure à  $A$ .

Il n'est pas nécessaire de nous arrêter à la démonstration de cette propriété bien connue; je me contente de faire remarquer que la démonstration repose en dernier lieu sur ce fait que la norme du produit de deux nombres complexes est égal au produit des normes des facteurs et que par conséquent lorsqu'on a

$$(x + yi)^n = p + qi,$$

même temps identiquement

$$(x^2 + y^2)^n = p^2 + q^2.$$

Il faut démontrer qu'il existe des valeurs (réelles) de  $x$  et de  $y$  qui satisfont simultanément  $u$  et  $v$ .

Or, si de telles valeurs n'existaient pas, l'expression

$$w = \log(u^2 + v^2)$$

serait une fonction de  $x$  et de  $y$  possédant les propriétés suivantes. En premier lieu, la fonction  $w$  serait finie et continue pour toutes les valeurs de  $x$  et de  $y$  et posséderait des dérivées partielles de tous les ordres par rapport à  $x$  et à  $y$ , lesquelles seraient également finies pour toutes les valeurs de  $x$  et de  $y$ .

En second lieu, la fonction  $w$  satisfait à l'équation

$$\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} = 0.$$

Il est évident si l'on songe que la fonction  $\frac{1}{2} \log(u^2 + v^2)$  est la partie réelle de la fonction  $\log f(z)$  de la variable complexe  $z$ . Mais on peut aussi le faire voir directement, car on sait que

$$\frac{\partial u}{\partial x} = \frac{\partial v}{\partial y}, \quad \frac{\partial u}{\partial y} = -\frac{\partial v}{\partial x}.$$

Or, on a

$$\frac{\partial w}{\partial x} = 2 \frac{u \frac{\partial u}{\partial x} + v \frac{\partial v}{\partial x}}{u^2 + v^2} = 2 \frac{u \frac{\partial v}{\partial y} - v \frac{\partial u}{\partial y}}{u^2 + v^2} = 2 \frac{\partial}{\partial y} \left( \arctg \frac{v}{u} \right),$$

$$\frac{\partial w}{\partial y} = 2 \frac{u \frac{\partial u}{\partial y} + v \frac{\partial v}{\partial y}}{u^2 + v^2} = 2 \frac{-u \frac{\partial v}{\partial x} + v \frac{\partial u}{\partial x}}{u^2 + v^2} = -2 \frac{\partial}{\partial x} \left( \arctg \frac{v}{u} \right).$$

Donc

$$\frac{\partial^2 w}{\partial x^2} + \frac{\partial^2 w}{\partial y^2} = 0.$$

Les fonctions possédant les mêmes propriétés que la fonction  $w$  sont appelées fonctions harmoniques. On en déduit un théorème qui — si l'on représente les variables  $x$  et  $y$  par les points d'un plan, dont  $x$  et  $y$  sont les coordonnées rectangulaires, — consiste en ceci : la valeur d'une fonction harmonique en un point quelconque est égale à la moyenne des valeurs qu'elle prend sur un cercle centré en ce point.

end cette fonction sur une circonférence de cercle dont le point considéré est le centre. On peut exprimer ce théorème plus nettement par la formule analytique suivante

$$w(x_0, y_0) = \frac{1}{2\pi} \int_0^{2\pi} w(x_0 + R \cos \varphi, y_0 + R \sin \varphi) d\varphi.$$

(Voir p. e. Riemann, Inaug. Diss., § 10, Gesamm. Werke, p 20.)

Mais cette relation conduit ici à une absurdité manifeste, car on peut toujours donner à  $R$  une grandeur telle que l'expression

$$w(x_0 + R \cos \varphi, y_0 + R \sin \varphi) = \log(u^2 + v^2)$$

est supérieure, pour toutes les valeurs de  $\varphi$ , à un nombre absolument arbitraire.

L'hypothèse qu'il n'existe pas de valeurs de  $x$  et de  $y$  annulant simultanément les fonctions  $u$  et  $v$  doit donc être fausse.

---

## XIV.

(Haarlem, Arch. Néerl. Sci. Soc. Holl, 18, 1883, 1—21.)

### Quelques considérations sur la fonction rationnelle entière d'une variable complexe.

1. Soit  $f(z) = z^n + A_1 z^{n-1} + A_2 z^{n-2} + \dots + A_n$  une expression rationnelle entière en  $z$ , du degré  $n$ .

La démonstration donnée par Cauchy pour le théorème fondamental de l'algèbre, démonstration qui à raison de sa simplicité est entrée dans divers traités élémentaires (Schlömilch, Compendium der höheren Analysis; v. d. Ven, Theorie en oplossing der hoogere wortsvergelijkingen), revient alors à ce qui suit.

En supposant qu'il ne fût pas possible de choisir  $x$  et  $y$  de telle sorte que, pour  $z = x + yi$ ,  $X$  et  $Y$  devinssent nuls simultanément

$$f(z) = X + Yi,$$

l'expression

$$X^2 + Y^2$$

pourrait pas non plus s'annuler pour aucun système de valeurs  $x$  et  $y$ .

Il en résulterait que cette expression devrait prendre, pour au moins un système de valeurs  $x$  et  $y$ , une valeur minima positive différente de zéro. Or, cela est impossible, car on fait voir que, quels que soient  $a$  et  $b$ , à la seule condition que pour  $x = a$ ,  $y = b$  l'expression  $X^2 + Y^2$  ne soit pas nulle,  $h$  et  $k$  peuvent toujours être déterminés de façon que, pour  $x = a + h$  et  $y = b + k$ ,  $X^2 + Y^2$  reçoive une valeur moindre que pour  $x = a$ ,  $y = b$ .



de la manière dont on établit ce fait, il résulte clairement aussi que  $\sqrt{X^2 + Y^2}$  ne peut pas non plus acquérir une valeur maxima, circonstance qui est d'ailleurs indifférente pour la démonstration de l'hy.

Puis  $\sqrt{X^2 + Y^2}$  est le module de  $f(z)$  et, lorsque  $a_1, a_2, \dots, a_n$  sont racines de l'équation  $f(z) = 0$ , égal au produit des distances de  $z$  à  $a_1, a_2, \dots, a_n$ .

Des simples réflexions suffisent donc pour montrer que la proposition plus d'une fois énoncée (voir, entre autres, Comptes rendus, t. 66, p. 288), que le module de  $f(z)$  prend aux points racines de

l'équation  $\frac{df(z)}{dz} = 0$  une valeur maxima ou minima, doit être inexacte.

Il est mieux en lumière les circonstances qui se produisent alors, c'est le but des premières considérations qui vont être développées, dans lesquelles je regarderai comme déjà prouvée la possibilité de la décomposition de  $f(z)$  en facteurs linéaires.

Exprimée sous une forme purement géométrique, la remarque précédente peut être énoncée en ces termes: étant donnés dans le plan  $n$  points fixes  $a_1, a_2, \dots, a_n$ , et en outre un point variable  $z$ , le produit des distances de  $z$  à  $a_1, a_2, \dots, a_n$  ne prend jamais une valeur maxima ou minima, sauf lorsque le point  $z$  coïncide avec un des points  $a_1, a_2, \dots, a_n$ . Plusieurs des points  $a_1, a_2, \dots, a_n$  peuvent d'ailleurs aussi coïncider entre eux.

Dans la démonstration suivante de cette proposition, il ne sera posé aucunement question de sa relation avec la théorie des fonctions algébriques.

Pour point de départ, je prends donc le développement en série du

$$\sqrt{1 - 2a \cos \varphi + a^2} = 1 - a \cos \varphi + \frac{1}{2} a^2 \cos 2\varphi - \dots = - \sum_{p=1}^{\infty} \frac{1}{p} a^p \cos p\varphi,$$

valable pour  $-1 < a < +1$  et pour des valeurs quelconques de  $\varphi$ . Ce développement peut servir de la manière suivante à comparer, entre elles, en deux points voisins, les valeurs du produit des distances de  $z$  à  $a_1, a_2, \dots, a_n$ .

Soient B et C ces deux points,  $r$  et  $\varphi$  les coordonnées polaires de C par rapport à un système d'axes ayant B pour origine,  $R_1$  et  $u_1$  les coordonnées polaires du point racine  $a_1$  par rapport à ce même système; on a alors

$$C a_1 = \sqrt{R_1^2 - 2 R_1 r \cos(\varphi - u_1) + r^2},$$

donc

$$\log C a_1 = \log R_1 + \log \sqrt{1 - 2 \frac{r}{R_1} \cos(\varphi - u_1) + \frac{r^2}{R_1^2}}.$$

En supposant  $r < R_1$ , on a donc, d'après (1),

$$\log C a_1 = \log B a_1 - \sum_{p=1}^{p=\infty} \frac{1}{p} \frac{r^p}{R_1^p} \cos p(\varphi - u_1).$$

Si  $R_2, u_2; R_3, u_3; \dots$  sont les coordonnées polaires de  $a_2, a_3, \dots$  dans le système d'axes adopté, et si  $r$  est plus petit que  $R_2, R_3, \dots$ , on a pareillement

$$\log C a_2 = \log B a_2 - \sum_{p=1}^{p=\infty} \frac{1}{p} \frac{r^p}{R_2^p} \cos p(\varphi - u_2)$$

$$\log C a_3 = \log B a_3 - \sum_{p=1}^{p=\infty} \frac{1}{p} \frac{r^p}{R_3^p} \cos p(\varphi - u_3)$$

. . . . .

et par l'addition de toutes ces équations nous obtenons

$$2) \quad \log(C a_1 \cdot C a_2 \dots C a_n) = \log(B a_1 \cdot B a_2 \dots B a_n) + \sum_{p=1}^{p=\infty} k_p r^p,$$

d'où

$$3) \quad k_p = -\frac{1}{p} \sum_{i=1}^{i=n} \frac{\cos p(\varphi - u_i)}{R_i^p}.$$

Puisque B est regardé, de même que  $a_1, a_2, \dots, a_n$ , comme fixe, C seul étant supposé variable, nous pouvons réduire  $k_p$  à une forme encore plus simple en posant

$$4) \quad \dots \dots \dots \begin{cases} M_p \cos \alpha_p = -\frac{1}{p} \sum_{i=1}^{i=n} \frac{\cos p u_i}{R_i^p}, \\ M_p \sin \alpha_p = -\frac{1}{p} \sum_{i=1}^{i=n} \frac{\sin p u_i}{R_i^p}; \end{cases}$$

$k_p$  et  $\alpha_p$  sont alors constants et il vient

$$k_p = M_p \cos(p\varphi - \alpha_p),$$

onc

$$\log(C a_1 \cdot C a_2 \dots C a_n) = \log(B a_1 \cdot B a_2 \dots B a_n) + M_1 r \cos(\varphi - \alpha_1) + \\ + M_2 r^2 \cos(2\varphi - \alpha_2) + M_3 r^3 \cos(3\varphi - \alpha_3) + \dots$$

Il doit toujours être satisfait ici à la condition que  $r$  soit moindre que  $R_1, R_2, \dots$ ; en d'autres termes, le point C doit être situé à l'intérieur du cercle qui a B pour centre et un rayon égal à la plus petite des distances  $R_1, R_2, \dots$ . Dans tout ceci, il est à peine besoin de le dire, on admet que B ne coïncide pas avec l'un des points  $a_1, a_2, \dots, a_n$ .

En ce qui concerne les nombres positifs  $M_1, M_2, M_3, \dots$ , on voit aisément qu'ils ne peuvent pas tous être égaux à zéro; mais il est très possible que quelques-uns des premiers soient nuls. Admettons que dans la suite  $M_1, M_2, \dots, M_s$  soit le premier nombre différent de zéro, et qu'on ait par conséquent

$$\log(C a_1 \cdot C a_2 \dots C a_n) = \log(B a_1 \cdot B a_2 \dots B a_n) + T, \\ T = M_s r^s \cos(s\varphi - \alpha_s) + M_{s+1} r^{s+1} \cos[(s+1)\varphi - \alpha_{s+1}] + \dots$$

Nous avons maintenant à rechercher comment la valeur de T varie avec le point C, c'est-à-dire, lorsque  $r$  et  $\varphi$  seuls prennent d'autres valeurs.

Remarquons d'abord que la série

$$M_s r^s + M_{s+1} r^{s+1} + M_{s+2} r^{s+2} + \dots$$

est également convergente, tant que  $r$  reste moindre que le plus petit des nombres  $R_1, R_2, \dots, R_n$ ; cela se déduit aisément de (4). Il en résulte que la série

$$s M_s \sqrt{\frac{1}{2}} - (s+1) M_{s+1} r - (s+2) M_{s+2} r^2 - (s+3) M_{s+3} r^3 - \dots$$

converge aussi pour ces valeurs de  $r$ , et comme, pour  $r=0$ , cette dernière série a pour somme la valeur positive  $s M_s \sqrt{\frac{1}{2}}$  différente de zéro, on pourra donner aussi à  $r$  une valeur, positive et différente de zéro, telle qu'on ait

$$s M_s \sqrt{\frac{1}{2}} - (s+1) M_{s+1} r - (s+2) M_{s+2} r^2 - \dots > 0.$$

Simultanément, on a alors

$$8) \quad \dots \quad M_s \sqrt{\frac{1}{2}} - M_{s+1} r - M_{s+2} r^2 - \dots > 0.$$

Supposons maintenant qu'en (6)  $r$  reçoive une valeur positive satisfaisant aux conditions (7) et (8), et faisons alors varier  $\varphi$  seul, de manière à considérer des points C situés sur un cercle de rayon  $r$  décrit autour de B.

De (6), il suit

$$\frac{dT}{d\varphi} = -s M_s r^s \sin(s\varphi - a_s) - (s+1) M_{s+1} r^{s+1} \sin[(s+1)\varphi - a_{s+1}] - \dots$$

et, par (7) et (8), on reconnaît immédiatement que, tant que la valeur absolue de  $\cos(s\varphi - a_s)$  n'est pas inférieure à  $\sqrt{\frac{1}{2}}$ , T a le même signe que  $\cos(s\varphi - a_s)$ . De même, tant que la valeur absolue de  $\sin(s\varphi - a_s)$  n'est pas inférieure à  $\sqrt{\frac{1}{2}}$ ,  $\frac{dT}{d\varphi}$  et  $\sin(s\varphi - a_s)$  ont des signes contraires.

Pour obtenir toutes les valeurs de T correspondant à une valeur déterminée de  $r$ , il suffit de donner à  $\varphi$ , à partir d'une valeur initiale quelconque, un accroissement égal à  $2\pi$ , ce qui fait croître  $s\varphi - a_s$  de la quantité  $2\pi s$ .

Distinguons, dans cet accroissement, les  $4s$  intervalles suivants

$$(1). \quad s\varphi - a_s \text{ de } -\frac{\pi}{4} \text{ à } +\frac{\pi}{4},$$

$$(2). \quad s\varphi - a_s \text{ de } +\frac{\pi}{4} \text{ à } +3\frac{\pi}{4},$$

$$(3). \quad s\varphi - a_s \text{ de } +3\frac{\pi}{4} \text{ à } +5\frac{\pi}{4},$$

$$\dots \dots \dots$$

enfin

$$(4s). \quad s\varphi - a_s \text{ de } (8s-3)\frac{\pi}{4} \text{ à } (8s-1)\frac{\pi}{4}.$$

Dans les premier, troisième, cinquième, ... intervalles, la valeur absolue de  $\cos(s\varphi - a_s)$  est plus grande que  $\sqrt{\frac{1}{2}}$ , et alternativement positive et négative. Par conséquent, dans les premier, cinquième, neuvième, ... intervalles, T est positif; dans les troisième, septième, ... intervalles, T est négatif.

Dans les deuxième, quatrième, sixième, ... intervalles, la valeur absolue de  $\sin(s\varphi - a_s)$  est plus grande que  $\sqrt{\frac{1}{2}}$ , et alternativement

ive et négative. Par conséquent, dans les deuxième, sixième, . . .  
 valles,  $\frac{dT}{dq}$  est partout négatif, dans les quatrième, huitième, . . .  
 valles, partout positif.

au commencement du second intervalle,  $T$  est positif pour  
 $sq - a_n = \frac{\pi}{4}$ , à la fin négatif pour  $sq - a_n = 3\frac{\pi}{4}$ , et dans tout l'in-

tervalle  $\frac{dT}{dq}$  est négatif;  $T$  devient donc, dans ce second intervalle,  
 une fois égal à zéro. A l'origine du quatrième intervalle,  $T$  est négatif,

et à sa fin positif, et dans tout l'intervalle  $\frac{dT}{dq}$  est positif.  $T$  devient  
 une fois égal à zéro, dans le quatrième intervalle, une fois égal à zéro, etc.

Il est évident que  $T$  s'annule pour 2  $s$  valeurs différentes de  $q$ , et  
 chaque fois il change de signe.

Or, on a  $Ca_1, Ca_2, \dots, Ca_n < Ba_1, Ba_2, \dots, Ba_n$ , suivant que  $T > 0$ ; il  
 résulte donc, de ce qui précède, qu'au voisinage du point  $B$  il y a  
 bien des points  $C$  pour lesquels  $Ca_1, Ca_2, \dots, Ca_n$  est plus grand  
 que  $Ba_1, Ba_2, \dots, Ba_n$ , que des points pour lesquels le premier produit  
 est plus petit que le second. D'un maximum ou d'un minimum de  
 $T$  au point  $B$ , il ne saurait donc être question. Mais le  
 point  $B$  a été pris tout à fait arbitrairement, sauf qu'il ne devait  
 coïncider avec aucun des points  $a_1, a_2, \dots, a_n$ ; ce qui a été dit au  
 § 1 se trouve donc démontré.

Les conditions (7) et (8) sont de telle nature que, lorsqu'elles  
 sont remplies par une certaine valeur positive de  $r$ , toutes les valeurs  
 plus petites y satisfont également. Or, il est facile de  
 voir qu'en prenant  $r$  suffisamment petit, on peut faire que les  
 valeurs de  $q$  pour lesquelles  $T$  devient  $= 0$  diffèrent aussi peu qu'on  
 désire des valeurs pour lesquelles  $\cos(sq - a_n)$  s'annule. Considé-  
 rons, par exemple, la racine située dans le second intervalle pour  
 laquelle  $sq - a_n$  est compris entre  $\frac{\pi}{4}$  et  $3\frac{\pi}{4}$ , et prenons deux va-  
 leurs  $q_1, q_2$ , telles qu'on ait

$$sq_1 - a_n < \frac{\pi}{2} < sq_2 - a_n,$$

différence  $\varphi_2 - \varphi_1$  pouvant d'ailleurs être aussi petite qu'on le veut.

Dans

$$T(\varphi_1) = M_s r^s \cos(s\varphi_2 - \alpha_s) + \dots$$

premier terme est alors positif, dans

$$T(\varphi_2) = M r^s \cos(s\varphi_2 - \alpha_s) + \dots$$

premier terme est négatif. On peut maintenant prendre  $r$  assez petit pour que  $T(\varphi_1)$  lui-même soit positif,  $T(\varphi_2)$  négatif, et pour que cela reste vrai quand  $r$  continue à décroître. Pour une pareille valeur de  $r$ , et pour toutes les valeurs plus petites, l'équation  $T(\varphi) = 0$  possède alors évidemment une racine entre  $\varphi_1$  et  $\varphi_2$ .

On voit donc que la ligne pour laquelle  $T = 0$ , a en B un point multiple d'ordre  $s$ . Les tangentes menées en B aux  $s$  branches forment entre elles des angles égaux à  $\frac{\pi}{s}$ . Un petit cercle, décrit autour de B, est divisé par la ligne  $T = 0$  en  $2s$  secteurs. A l'intérieur de chaque secteur,  $T$  conserve le même signe, et dans les secteurs successifs, est alternativement positif et négatif.

La condition  $T = 0$  est équivalente à  $C a_1 \cdot C a_2 \dots C a_n = B a_1 \cdot B a_2 \dots B a_n$ . Si le point B est choisi arbitrairement,  $M_1$  ne sera pas, en général, égal à zéro; dans les considérations qui précèdent, on a alors  $M_1 = 1$ , et B est un point simple de la courbe  $C a_1 \cdot C a_2 \dots C a_n = B a_1 \cdot B a_2 \dots B a_n$ .

4. Pour découvrir la signification des conditions  $M_1 = 0, M_2 = 0, \dots$  convient de se reporter de nouveau à la théorie des équations algébriques.

A cet effet, introduisons un nouveau système d'axes rectangulaires, où l'axe des  $x$  soit parallèle à la droite à partir de laquelle les angles sont comptés dans le système polaire, ayant pour origine le point B dont nous nous sommes servis jusqu'ici, et où les directions des axes des  $x$  et  $y$  positifs correspondent à  $\varphi = 0$  et  $\varphi = 90^\circ$ . Soient  $x$  et  $y$  les coordonnées de B dans ce nouveau système, et  $z = x + yi$  une quantité variable complexe. Les points  $a_1, a_2, \dots$  peuvent alors représenter les nombres complexes  $z_1, z_2, \dots$ , C le nombre  $z + t$ , de sorte que  $t = r(\cos \varphi + i \sin \varphi)$ .

oit enfin

$$f(z) = (z - z_1)(z - z_2) \dots (z - z_n),$$

la résulte

$$\log f(z+t) = \log f(z) + \log \left(1 + \frac{t}{z-z_1}\right) + \log \left(1 + \frac{t}{z-z_2}\right) + \dots + \log \left(1 + \frac{t}{z-z_n}\right)$$

lorsque  $\text{mod } t$  est plus petit que les modules de  $z - z_1, z - z_2, \dots, z - z_n$ ,

$$\begin{aligned} \log f(z+t) = \log f(z) + & t \left( \frac{1}{z-z_1} + \frac{1}{z-z_2} + \dots + \frac{1}{z-z_n} \right) \\ & - \frac{1}{2} t^2 \left( \frac{1}{(z-z_1)^2} + \frac{1}{(z-z_2)^2} + \dots + \frac{1}{(z-z_n)^2} \right) \\ & + \frac{1}{3} t^3 \left( \frac{1}{(z-z_1)^3} + \frac{1}{(z-z_2)^3} + \dots + \frac{1}{(z-z_n)^3} \right) \\ & \dots \dots \dots \end{aligned}$$

on a

$$z - z_1 = -R_1 (\cos u_1 + i \sin u_1), \quad z - z_2 = -R_2 (\cos u_2 + i \sin u_2), \dots$$

l'on déduit, pour le coefficient de  $t^p$  dans (9)

$$(-1)^{p-1} \frac{1}{p} \sum_{i=1}^{i=n} \frac{1}{(z-z_i)^p} = -\frac{1}{p} \sum_{i=1}^{i=n} \frac{\cos p u_i - i \sin p u_i}{R_i^p}.$$

l'expression à droite est, d'après (4), égale à

$$M_p (\cos \alpha_p - i \sin \alpha_p).$$

donc on pose encore  $t = r (\cos \varphi + i \sin \varphi)$ , on obtient, en égalant les parties réelles des deux membres de (9)

$$\log \text{mod } f(z+t) = \log \text{mod } f(z) + M_1 r \cos (\varphi - \alpha_1) + M_2 r^2 \cos (2\varphi - \alpha_2) + \dots$$

qui est le développement en série du  $n^0 2$ .

Comme d'ailleurs la formule (1) résulte de

$$\log (1-z) = -z - \frac{1}{2} z^2 - \frac{1}{3} z^3 - \dots$$

si on y pose  $z = a e^{p i}$  et qu'on compare les parties réelles, ce mode de déduction ne diffère pas essentiellement de celui qui a été employé précédemment.

Il ressort maintenant que  $M_1, M_2, M_3, \dots$  sont les modules des coefficients des puissances de  $t$  dans (9). Si l'on pose

$$\frac{1}{z-z_1} + \frac{1}{z-z_2} + \dots + \frac{1}{z-z_n} = \psi(z),$$

ient

$$\log f(z+t) = \log f(z) + \psi(z)t + \frac{1}{2} \psi'(z)t^2 + \frac{1}{2 \cdot 3} \psi''(z)t^3 + \dots$$

$M_1, M_2, \dots$  sont les modules de  $\psi(z), \frac{1}{2} \psi'(z), \dots$

Or, on a

$$f'(z) = \psi(z)f(z),$$

il suit

$$f''(z) = \psi'(z)f(z) + \psi(z)f'(z),$$

$$f'''(z) = \psi''(z)f(z) + 2\psi'(z)f'(z) + \psi(z)f''(z),$$

$$f^{(4)}(z) = \psi'''(z)f(z) + 3\psi''(z)f'(z) + 3\psi'(z)f''(z) + \psi(z)f'''(z),$$

.....

l'on a donc  $M_1=0, M_2=0, \dots, M_{s-1}=0$  et  $M_s$  non égal à zéro,  $f'(z), \dots, f^{(s-1)}(z)$  sont également nuls et  $f^{(s)}(z)$  n'est pas nul; d'autres termes,  $z$  est une racine multiple de l'ordre  $s-1$  de l'équation  $f'(z)=0$ . Et réciproquement: lorsque  $z$  est une racine multiple de l'ordre  $s-1$  de  $f'(z)=0$ , les quantités  $M_1, M_2, \dots, M_{s-1}$  sont égales à zéro et  $M_s$  n'est pas égal à zéro.

D'après ce qui a été dit au n° 3, on voit donc maintenant que les points multiples des courbes pour lesquelles on a  $\text{mod } f(z) = C$  coïncident avec les racines de  $f'(z)=0$ ; et c'est seulement pour des valeurs particulières de  $C$ , en nombre tout au plus égal à  $n-1$ , que la courbe  $\text{mod } f(z) = C$  a de pareils points multiples. Quant à d'autres espèces de points singuliers, elle n'en possède pas, d'après ce qui a été dit au n° 2.

Ce qui précède nous met en état d'obtenir une idée générale de l'allure des courbes

$$\text{mod } f(z) = \text{Constante.}$$

Faisons d'abord quelques remarques.

Lorsque, à la limite d'un domaine (fini) continu,  $\text{mod } f(z)$  prend une valeur constante, il faut qu'au moins une des racines  $a_1, \dots, a_n$  soit située à l'intérieur de ce domaine, et que  $\text{mod } f(z)$



pour les points intérieurs au domaine une valeur plus petite que sur le contour. En effet, puisque  $\text{mod } f(z)$  varie continuellement, il doit prendre au moins en un point sa valeur minimum en un autre point sa valeur maximum. Le minimum ne peut pas se trouver au bord du domaine, car alors le maximum se trouverait à l'intérieur, ce qui, d'après le n° 2, n'est pas possible. Les minima existent donc en dedans du domaine et nous savons que ces minima existent qu'aux points racines. La valeur marginale, au contraire, est le maximum de  $\text{mod } f(z)$ , et les valeurs de  $\text{mod } f(z)$  à l'intérieur du domaine sont plus petites que cette valeur marginale. De là, nous pouvons conclure :

2°. Qu'un domaine continu, à la limite duquel  $\text{mod } f(z)$  est constant, est nécessairement simplement connexe. Car si  $\text{mod } f(z)$  avait, par exemple, la même valeur constante sur le contour du domaine doublement connexe  $T$ , il en résulterait, d'après ce qui précède, que, tant en  $T$  qu'en  $T_1$ , la valeur de  $\text{mod } f(z)$  serait moindre qu'aux points de  $C_1$ . Or cela ne se peut pas, car, suivant le n° 2, la courbe le long de laquelle  $\text{mod } f(z)$  a une valeur constante forme la séparation entre un domaine dans lequel  $\text{mod } f(z)$  a une valeur plus petite et un autre domaine, dans lequel  $\text{mod } f(z)$  a une valeur plus grande.

Après tout ce qui précède, il est évident que :

3°. Si nous isolons un domaine quelconque, mais entièrement limité, qui ne contienne aucune des racines, les maxima et minima de  $\text{mod } f(z)$ , pour ce domaine, devront être cherchés au bord du domaine.

Rappelons enfin que,

4°. lorsque  $\text{mod } z$  croît indéfiniment,  $\text{mod } f(z)$  finit aussi par croître indéfiniment, au-delà de toute limite.

3. Pour que le cas où l'équation  $f(z) = 0$  possède des racines multiples soit également compris dans la démonstration, nous supposons que  $z_1, z_2, \dots, z_k$  soient les racines non égales de  $f(z) = 0$ .

Si  $k < n$ , les autres racines,  $z_{k+1}, \dots, z_n$ , ne sont donc que des répétitions de  $z_1, z_2, \dots, z_k$ .

L'équation  $f'(z) = 0$  a alors  $k - 1$  racines

$$(10) \quad y_1, y_2, \dots, y_{k-1}$$

dont aucune ne coïncide avec  $z_1, z_2, \dots, z_k$  et qui peuvent être représentées par les points  $B_1, B_2, \dots, B_{k-1}$ . Les autres racines de  $f'(z) = 0$  sont en même temps racines de  $f(z) = 0$ . Il est très possible, toutefois, que parmi les racines  $y_1, y_2, \dots, y_{k-1}$  il y en ait d'égales, et nous mentionnons expressément que de pareilles racines doivent être censées inscrites en (10) autant de fois que l'indique le degré de la multiplicité.

Soit, en outre,

$$\text{mod } f(y_1) = c_1, \text{ mod } f(y_2) = c_2, \dots, \text{ mod } f(y_{k-1}) = c_{k-1};$$

les constantes  $c_1, c_2, \dots$  sont donc positives et différentes de zéro. Comme l'ordre de succession des racines est arbitraire, nous pouvons supposer

$$c_1 \leq c_2 \leq c_3 \dots \leq c_{k-1}.$$

Il convient de remarquer encore qu'on peut avoir, par exemple,  $c_1 = c_2$ , sans que, pour cela  $y_1 = y_2$ . Si par exemple,  $f(z) = z^n + A_1 z^{n-1} + \dots$  a des coefficients réels, et que  $y_1, y_2$  soient des racines complexes, conjuguées, de  $f'(z) = 0$ , on a évidemment  $c_1 = c_2$ .

7. Les courbes pour lesquelles on a  $\text{mod } f'(z) = C$  seront maintenant considérées comme les limites du domaine où  $\text{mod } f(z)$  est moindre que  $C$ . Lorsque  $C$  croît, ce domaine s'étend donc progressivement, de sorte que le domaine correspondant à une plus petite valeur de  $C$  forme toujours une partie du domaine qui appartient à une plus grande valeur de  $C$ . Pour  $C = 0$ , il n'y a que les  $k$  points isolés  $A_1, A_2, \dots, A_k$  qui satisfassent à la condition  $\text{mod } f(z) = 0$ .

Il est ensuite facile de montrer que, pour des valeurs suffisamment petites de  $C$ , le domaine

$$\text{mod } f(z) \leq C$$

se compose de  $k$  aires continues, entièrement isolées les unes des autres, dont chacune renferme un des points  $A_1, A_2, \dots, A_k$ , de

entourent les racines  $A_1, A_2, \dots, A_k$ .

Décrivons en effet, autour de  $A_1, A_2, \dots, A_k$ , des cercles  $K_1, K_2, \dots, K_k$ , entièrement isolés les uns des autres, et soit  $m$  la valeur minimum de  $\text{mod } f(z)$  sur la circonférence de ces cercles. Pour chaque point  $P$  en dehors de ces cercles, on a alors  $\text{mod } f(z) > m$ . Pour s'en convaincre, on n'a qu'à considérer le cercle  $K$  où  $\text{mod } z$  a une valeur constante, et qui, en même temps, satisfait aux conditions

- 1°: d'entourer le point  $P$  et tous les cercles  $K_1, \dots, K_k$ ,
- 2°: que le minimum de  $\text{mod } f(z)$  pour les points du cercle soit plus grand que  $m$ . Il est clair, d'après le n° 5, qu'il existe toujours un pareil cercle.

Du n° 5, 3°, il résulte alors que  $m$  est le minimum des valeurs de  $\text{mod } f(z)$  situées dans le domaine en dehors de  $K_1, K_2, \dots, K_k$  et à l'intérieur de  $K$ , de sorte que le module de  $f(z)$  en  $P$  est plus grand que  $m$ .

Lorsque  $C < m$ , le domaine où l'on a

$$\text{mod } f(z) \leq C$$

ne contient donc aucun point situé en dehors des cercles  $K_1, K_2, \dots, K_k$ . D'autre part, il est clair que  $A_1, A_2, \dots, A_k$  appartiennent à ce domaine, et du n° 5, 1° et 2°, il suit donc que le domaine  $\text{mod } f(z) \leq C$  est composé de  $k$  aires continues isolées, dont le contour consiste par conséquent en  $k$  courbes fermées. Aucune de ces courbes ne peut se couper elle-même.

Si  $C$  croît, chacune de ces  $k$  aires continues s'étendra, jusqu'à ce que  $C$  atteigne la valeur  $c_1$ . Supposons d'abord  $c_1 < c_2$ , la courbe  $\text{mod } f(z) = c_1$  a alors, d'après le n° 2, en  $B_1$  un point double, et les deux branches se coupent à angle droit. Décrivons autour de  $B_1$  comme centre, avec un rayon suffisamment petit, un cercle; celui-ci sera divisé en quatre secteurs  $S_1, S_2, S_3, S_4$ .

Soit, dans les secteurs  $S_1, S_3$ ,  $\text{mod } f(z) < c_1$ , dans les secteurs  $S_2, S_4$ ,  $\text{mod } f(z) > c_1$ .

Si  $h$  est une quantité positive suffisamment petite, le domaine  $\text{mod } f(z) \leq c_1 - h$  s'étendra donc dans  $S_1$  et  $S_3$  mais non jusqu'au point

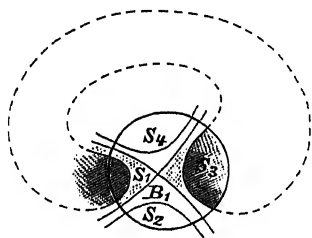
$B_1$ , de sorte que ces aires ne se réunissent point à l'intérieur du cercle. La courbe  $\text{mod } f(z) = c_1 + h$ , au contraire, pénètre dans  $S_2$  et  $S_4$ , et la partie du domaine  $\text{mod } f(z) = c_1 + h$ , située à l'intérieur du cercle, est continue.

Ainsi, au moment où  $C$  dépasse la valeur  $c_1$ , deux aires séparées du domaine  $\text{mod } f(z) \leq C$  se réunissent. Le nombre des aires continues distinctes du domaine

$$\text{mod } f(z) \leq C$$

est donc pour  $C = c_1 + h$  égal à  $k - 1$ . Cette conclusion suppose, toutefois, que les deux aires de  $\text{mod } f(z) \leq c_1 - h$  qui pénètrent à

l'intérieur du cercle ne s'unissent pas non plus entre elles dans leur prolongement en dehors du cercle (comme il arriverait, par exemple, si ce prolongement avait lieu de la manière indiquée, dans la figure, par des lignes pointillées).



On reconnaît de suite que tel est réellement le cas, en réfléchissant que, s'il en était autrement, il en résulterait évidemment un domaine doublement connexe sur le contour duquel on aurait  $\text{mod } f(z) = c_1 + h$ , ce qui, d'après le n° 5, 2° n'est pas possible.

Si l'on a  $y_1 = y_2$ , de sorte que les points  $B_1, B_2$  coïncident, on a aussi  $c_1 = c_2$  et  $B_1$  est un point triple de la courbe  $\text{mod } f(z) = c_1$ ; un cercle suffisamment petit, décrit autour de  $B_1$ , est alors partagé en six secteurs, à l'intérieur desquels  $\text{mod } f(z)$  est alternativement plus grand et plus petit que  $c_1$ .

On voit facilement que, dans ce cas, le nombre des aires distinctes du domaine  $\text{mod } f(z) < C$  diminue de deux unités au moment où la valeur  $c_1 = c_2$  est dépassée.

Il en est de même lorsqu'on a  $c_1 = c_2$  sans avoir  $y_1 = y_2$ .

Si donc on a  $C < c_{k-1}$ , la ligne  $\text{mod } f(z) = C$  consiste en une courbe fermée unique, qui entoure toutes les racines. Comme règle générale, on peut établir que, lorsque  $C$  n'est pas égal à l'une des constantes  $c_1, c_2, \dots, c_{k-1}$ , et que  $t$  de ces constantes sont plus grandes que  $C$ , la ligne

$$\text{mod } f(z) = C$$

se compose de  $t + 1$  courbes fermées, isolées les unes des autres, qui ensemble, entourent toutes les racines  $A_1, A_1, \dots, A_k$ .

8. Pour éclaircir ce qui précède, je choisirai l'exemple

$$f(z) = z^4 + z^3 - 2.$$

On a alors

$$z_1 = +1,$$

$$z_2 = -1.5437,$$

$$z_3 = -0.2282 + 1.1151 i,$$

$$z_4 = -0.2282 - 1.1151 i;$$

puis

$$f'(z) = 4z^3 + 3z^2,$$

$$y_1 = 0, \quad c_1 = 2,$$

$$y_2 = 0, \quad c_2 = 2,$$

$$y_3 = -\frac{3}{4}, \quad c_3 = 2\frac{27}{56}.$$

Il s'agit maintenant de déterminer, sur les lignes

$$\text{mod } f(z) = 2,$$

$$\text{mod } f(z) = 2\frac{27}{56},$$

un nombre de points suffisants pour que leur allure se dessine clairement.

En ce qui concerne la première de ces lignes, puisque  $\text{mod } f(z) = 2$  on doit avoir

$$f(z) = 2(\cos \alpha + i \sin \alpha).$$

J'ai donc, pour différentes valeurs de  $\alpha$ , calculé chaque fois les quatre racines de cette équation du quatrième degré. Comme le changement de  $\alpha$  en  $-\alpha$  fait manifestement passer  $z$  à sa valeur conjuguée, il suffisait de prendre  $\alpha$  entre 0 et 180°. De cette manière ont été

les racines lorsque  $\alpha$  approche de  $180^\circ$ , il était nécessaire de calculer encore quelques autres points de la ligne  $\text{mod } f(z) = 2$ ; mais, pour ceux-là, il eût été moins convenable de conserver  $\alpha$  pour argument. Aussi les valeurs données dans le tableau Ia ont-elles été trouvées d'une autre manière.

On a opéré de même pour la ligne  $\text{mod } f(z) = 2\frac{27}{56}$ .

Dans le tableau II, sont indiquées les racines de l'équation

$$f(z) = 2\frac{27}{56}(\cos \alpha + i \sin \alpha),$$

tandis que le tableau IIa fait encore connaître quelques autres points de la ligne  $\text{mod } f(z) = 2\frac{27}{56}$ .

La figure ci-contre donne une idée suffisante de la forme de ces courbes, qui, au moyen des valeurs consignées dans les tableaux, pourraient être représentées avec encore plus d'exactitude sur un dessin à échelle moins réduite.

Si l'on a  $C < 2$ , la ligne

$$\text{mod } f(z) = C$$

est composée de 4 courbes fermées entourant  $A_1, A_2, A_3, A_4$ .

Dans le cas de  $2 < C < 2\frac{27}{56}$ , la ligne est composée de deux courbes fermées, dont l'une entoure  $A_1, A_3, A_4$ , l'autre,  $A_2$ . Pour  $C > 2\frac{27}{56}$  la ligne consiste en une seule courbe fermée, qui enveloppe tous les points  $A_1, A_2, A_3, A_4$ .

9. Considérons encore une fois, pour une valeur quelconque de  $C$ , la ligne  $\text{mod } f(z) = C$ . Cette ligne se compose alors d'un certain nombre de courbes fermées

$$K_1, K_2, \dots, K_s$$

qui n'ont pas de points communs et à l'intérieur desquelles sont situées toutes les racines  $A_1, A_2, \dots, A_k$ . Lors même que ces lignes, pour certaines valeurs particulières de  $C$ , auraient entré

sidère comme les limites du domaine où  $\text{mod } f(z)$  est  $< C$ , n'en serait pas moins complètement déterminé.

Désignons par  $n_1, n_2, \dots, n_s$  les nombres des racines de  $f(z) = 0$  qui sont situées à l'intérieur de  $K_1, K_2, \dots, K_s$ , de sorte qu'on ait

$$n_1 + n_2 + \dots + n_s = n,$$

les racines égales étant comptées d'après le degré de leur multiplicité.

Si maintenant la variable  $z$  parcourt la ligne entière  $K_1$ , de manière à retomber finalement sur sa valeur initiale,  $f(z)$  prend des valeurs dont le module est égal à  $C$ , et pour  $f(z) = C(\cos \varphi + i \sin \varphi)$  l'argument  $\varphi$  de  $f(z)$  croît de  $2n_1\pi$ , puisqu'à l'intérieur de  $K_1$  il y a  $n_1$  racines de  $f(z) = 0$ . Il en résulte, évidemment, que l'expression  $f(z)$  prend alors toutes les valeurs ayant  $C$  pour module, et qu'elle prend chacune de ces valeurs au moins  $n_1$  fois.

Pareillement, si  $z$  parcourt la ligne  $K_2$ , l'expression  $f(z)$  prend toutes les valeurs ayant  $C$  pour module, et elle prend chacune de ces valeurs au moins  $n_2$  fois, etc.

Si l'on fait donc parcourir à  $z$  successivement toutes les lignes  $K_1, K_2, \dots, K_s$ , et que

$$t = C(\cos u + i \sin u)$$

soit un nombre quelconque avec  $C$  pour module,  $f(z)$  prendra au moins  $n_1 + n_2 + \dots + n_s$  fois, c'est-à-dire au moins  $n$  fois, la valeur  $f(z) = t$ . Mais comme l'équation  $f(z) = t$  n'a pas plus de  $n$  racines, il est clair qu'il n'y a pas plus de  $n_1$ , mais justement  $n_1$  racines de l'équation  $f(z) = t$  situées sur la ligne  $K_1$ ; de même, sur les lignes  $K_2, K_3, \dots$ , se trouvent respectivement  $n_2, n_3, \dots$  racines de cette équation.

On voit en outre, immédiatement, que lorsque le module de  $t'$  est plus petit que  $C$ , il y a à l'intérieur de  $K_1, K_2, \dots$  respectivement  $n_1, n_2, \dots$  points où  $f(z)$  prend la valeur  $t'$ .

Le cas particulier où la ligne  $K_1$  ne renferme qu'une seule racine, mérite d'être remarqué. Si on a alors  $\text{mod } t' \leq C$ , il n'y a à l'intérieur de  $K_1$  qu'un seul point où  $f(z)$  prenne la valeur  $t'$ , et lorsque  $t_1, t_2$  sont deux points, non coïncidents, situés à l'intérieur de  $K_1$ ,  $f(t_1)$  n'est jamais égal à  $f(t_2)$ .

$Z_1$		$Z_2$		$Z_3$		$Z_4$	
$x_1$	$y_1$	$x_2$	$y_2$	$x_3$	$y_3$	$x_4$	
+ 1.2173	0.0000	— 1.7484	0.0000	— 0.2345	+ 1.3507	— 0.2345	—
1.2157	+ 0.0299	1.7468	— 0.0286	0.2665	1.3483	0.2024	
1.2107	0.0596	1.7419	0.0569	0.2984	1.3424	0.1704	
1.2025	0.0889	1.7338	0.0848	0.3298	1.3330	0.1388	
1.1908	0.1176	1.7223	0.1121	0.3606	1.3201	0.1078	
1.1757	0.1456	1.7075	0.1386	0.3907	1.3034	0.0774	
1.1571	0.1724	1.6893	0.1639	0.4197	1.2830	0.0481	
1.1347	0.1980	1.6675	0.1878	0.4474	1.2587	— 0.0198	
1.1086	0.2221	1.6420	0.2101	0.4736	1.2301	+ 0.0070	
1.0783	0.2443	1.6125	0.2304	0.4979	1.1970	0.0321	
1.0436	0.2643	1.5789	0.2482	0.5200	1.1590	0.0553	
1.0040	0.2816	1.5405	0.2629	0.5394	1.1153	0.0760	
0.9587	0.2956	1.4969	0.2740	0.5556	1.0650	0.0938	
0.9065	0.3056	1.4471	0.2804	0.5676	1.0066	0.1082	
0.8457	0.3103	1.3896	0.2806	0.5740	0.9375	0.1180	
0.7727	0.3078	1.3219	0.2717	0.5726	0.8532	0.1218	
0.6804	0.2939	1.2389	0.2479	0.5582	0.7433	0.1168	
0.5481	0.2577	1.1295	0.1922	0.5142	0.5773	0.0957	
0.0000	0.0000	1.0000	0.0000	0.0000	0.0000	0.0000	

Tableau Ia.

$Z_1$		$Z_2$		$Z_3$		$Z_4$	
$x_1$	$y_1$	$x_2$	$y_2$	$x_3$	$y_3$	$x_4$	
+ 0.5427	+ 0.2559	— 1.0733	— 0.1474	— 0.4407	+ 0.4071	+ 0.0864	—
0.4485	0.2210	1.0275	0.0913	0.3856	0.3183	0.0662	
0.3563	0.1818	1.0038	0.0342	0.3208	0.2389	0.0459	
0.2655	0.1396			0.2476	0.1694	0.0275	
0.1759	0.0952			0.1687	0.1074	0.0128	
0.0873	0.0487			0.0856	0.0516	0.0033	



$Z_1$		$Z_2$		$Z_3$		$Z_4$	
$x_1$	$y_1$	$x_2$	$y_2$	$x_3$	$y_3$	$x_4$	$y_4$
+ 1.2263	0.0000	— 1.7570	0.0000	— 0.2347	+ 1.3603	— 0.2347	— 1.3603
1.2246	+ 0.0309	1.7553	— 0.0295	0.2678	1.3579	0.2015	1.3579
1.2196	0.0616	1.7503	0.0588	0.3006	1.3519	0.1686	1.3519
1.2111	0.0919	1.7421	0.0878	0.3331	1.3424	0.1359	1.3424
1.1993	0.1216	1.7304	0.1160	0.3650	1.3292	0.1038	1.3292
1.1839	0.1506	1.7153	0.1435	0.3962	1.3123	0.0724	1.3123
1.1649	0.1785	1.6967	0.1698	0.4263	1.2916	0.0419	1.2916
1.1422	0.2052	1.6745	0.1949	0.4552	1.2668	— 0.0125	1.2668
1.1156	0.2305	1.6485	0.2183	0.4827	1.2378	+ 0.0156	1.2378
1.0847	0.2539	1.6183	0.2397	0.5084	1.2041	0.0420	1.2041
1.0494	0.2753	1.5839	0.2589	0.5321	1.1653	0.0667	1.1653
1.0089	0.2942	1.5446	0.2751	0.5534	1.1208	0.0891	1.1208
0.9625	0.3101	1.4998	0.2879	0.5716	1.0695	0.1089	1.0695
0.9091	0.3224	1.4485	0.2964	0.5864	1.0099	0.1258	1.0099
0.8466	0.3301	1.3890	0.2992	0.5966	0.9391	0.1390	0.9391
0.7714	0.3320	1.3182	0.2941	0.6010	0.8523	0.1478	0.8523
0.6756	0.3260	1.2299	0.2766	0.5972	0.7384	0.1515	0.7384
0.5367	0.3097	1.1068	0.2343	0.5826	0.5632	0.1527	0.5632
0.2500	0.3536	0.7500	0.0000	0.7500	0.0000	0.2500	0.0000

T a b l e a u IIa.

$Z_1$		$Z_2$		$Z_3$		$Z_4$	
$x_1$	$y_1$	$x_2$	$y_2$	$x_3$	$y_3$	$x_4$	$y_4$
+ 0.4315	+ 0.3021	— 0.9832	— 0.1734	— 0.5896	+ 0.6434	+ 0.1585	— 0.1585
0.3650	0.3063	0.8938	0.1177	0.5775	0.4846	0.1734	0.1734
0.3174	0.3174	0.8326	0.0728	0.5766	0.4038	0.1959	0.1959
0.2799	0.3335			0.5815	0.3357	0.2209	0.2209
				0.5917	0.2759		
				0.6071	0.2209		
				0.6283	0.1684		
				0.6569	0.1158		
				0.6956	0.0609		

## XV.

(Zs. Vermessgsw. Stuttgart., 15, 1886, 141—144.)

### Möglichkeit oder Unmöglichkeit einer Pothenotischen Bestimmung <sup>1)</sup>.

Um das Kriterium der Möglichkeit einfach darzustellen, nenne ich das gegebene Dreieck ABC Fig. 1. und Fig. 2. und zugleich sollen die Winkel dieses Dreiecks bezeichnet werden:

$$BAC = A, CBA = B, ACB = C,$$

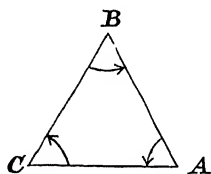


Fig. 1.

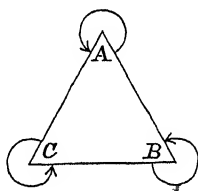


Fig. 2.

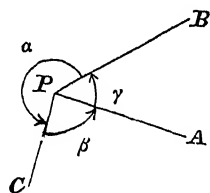


Fig. 3.

doch muss noch der Drehungssinn festgesetzt werden, damit dieser Winkel eindeutig bestimmt seien. Dieser Drehungssinn für die Winkelmessung soll so angenommen werden, wie der Sehstrahl PA beim Uebergang nach PC gedreht werden muss, ohne PA zu treffen. In diesem Sinne sei nach Fig. 3.

$$\text{Winkel } BPC = \alpha,$$

$$\text{„ } CPA = \beta,$$

$$\text{„ } APB = \gamma.$$

Die Winkel  $\alpha$ ,  $\beta$ ,  $\gamma$  werden hiernach zwischen  $0^\circ$  und  $360^\circ$  liegen

lass sie entweder das sind, was man schlechterdings unter Winkeln eines Dreiecks versteht, so dass

$$A + B + C = 180^\circ,$$

oder es sind A, B, C Winkel, welche, zu den gewöhnlichen Winkeln des Dreiecks addirt, jedesmal  $360^\circ$  geben, so dass

$$A + B + C = 900^\circ.$$

Der erste Fall trifft dann ein, wenn der Drehungssinn der Winkel mit dem des Dreiecks ABC übereinstimmt, der zweite Fall tritt ein, wenn dies nicht der Fall ist. Was hiernach unter Drehungssinn eines Dreiecks ABC zu verstehen ist, wird einleuchtend sein.

Fig. 1. hat negativen Drehungssinn, Fig. 2. hat positiven Drehungssinn. Nach diesen Festsetzungen betreffs der Winkel

$$\alpha, \beta, \gamma \quad A, B, C$$

kann man Folgendes sagen:

Die Pothenotische Aufgabe ist physisch möglich oder unmöglich je nachdem von den drei Differenzen

$$\alpha - A, \beta - B, \gamma - C$$

eine *gerade* (0 oder 2) oder eine *ungerade* (1 oder 3) Anzahl *negativer* ist. Sollte *eine* der Differenzen  $\alpha - A, \beta - B, \gamma - C$  Null sein, so ist die Aufgabe unmöglich (selbst nach Vertauschung einer Richtung mit der entgegengesetzten), sind *zwei* Null, so ist die Aufgabe gänzlich unbestimmt, und der gesuchte Punkt kann willkürlich auf einem Bogen des um ABC beschriebenen Kreises genommen werden (Alle drei Differenzen können nicht Null werden, da ihre Summe ja keinesfalls gleich Null ist)

Die Bestimmung der Winkel A, B, C wird zweideutig, wenn die drei Punkte ABC auf einer Geraden liegen. Nehmen wir z. B. für B den mittlern Punkt, so findet man in diesem Fall:

$$\begin{array}{ll} \text{entweder } A = 0^\circ, & \text{oder } A = 360^\circ, \\ B = 180^\circ, & B = 180^\circ, \\ C = 0^\circ, & C = 360^\circ, \end{array}$$

entsprechend der Unbestimmtheit des Drehungssinnes des Dreiecks

ABC. Diese Zweideutigkeit hat jedoch *keinen* Einfl  
gegebene Kriterium, denn man hat zu untersuchen

$$\begin{array}{ccc} \alpha, & \text{oder} & \alpha - 360^\circ, \\ \beta - 180^\circ, & & \beta - 180^\circ, \\ \gamma, & & \gamma - 360^\circ \end{array}$$

und da  $\alpha > 0$ ,  $\gamma > 0$ ,  $\alpha - 360^\circ < 0$ ,  $\gamma - 360^\circ < 0$ , so fin  
einen wie in dem anderen Falle immer, dass die A

$$\begin{array}{ll} \text{möglich für} & \beta > 180^\circ, \\ \text{unmöglich für} & \beta < 180^\circ \text{ ist,} \end{array}$$

wie auch leicht unmittelbar einzusehen ist.

---

## XVI.

(Bul. Sci. Math., Paris, sér. 2, 7, 1883, 139—142.)

---

### Sur la théorie des résidus biquadratiques.

(Extrait d'une Lettre adressée à M. Hermite.)

Vous savez que, dans son second Mémoire, Gauss a déterminé le caractère biquadratique du nombre  $1 + i$  par rapport à un nombre premier  $M$ , ou, d'après Jacobi, la valeur du symbole  $\left(\left(\frac{1+i}{M}\right)\right)$ . Cette détermination se fonde sur le théorème de l'art 71, théorème analogue à celui qui sert de fondement à la troisième et à la cinquième des démonstrations de Gauss, de la loi de réciprocité pour les résidus quadratiques.

Or j'ai remarqué qu'on peut obtenir la valeur de  $\left(\left(\frac{1+i}{M}\right)\right)$  à l'aide de raisonnements complètement analogues à ceux que Gauss développe dans son premier Mémoire, pour obtenir le caractère du nombre 2 dans la théorie réelle.

Il suffira de considérer le cas

$$M = a + bi, \quad a \equiv 1 \pmod{4},$$

$$b \equiv 0, \quad \mu = aa + bb = 8n + 1.$$

$$(B) \quad \beta, \beta', \beta'', \dots \left( \left( \frac{\beta}{M} \right) \right) = i,$$

$$(C) \quad \gamma, \gamma', \gamma'', \dots \left( \left( \frac{\gamma}{M} \right) \right) = -1,$$

$$(D) \quad \delta, \delta', \delta'', \dots \left( \left( \frac{\delta}{M} \right) \right) = -i.$$

Alors est évident qu'on a identiquement

$$(x - \delta)(x - \delta')(x - \delta'') \dots \equiv x^{\frac{\mu-1}{4}} + i \pmod{M},$$

d'où l'on tire, en posant  $x = -1$ ,

$$(1 + \delta)(1 + \delta')(1 + \delta'') \dots \equiv 1 + i \pmod{M};$$

ce qui fait voir qu'il suffira de savoir combien des nombres  $1 + \delta, 1 + \delta', 1 + \delta'', \dots$  appartiennent aux classes (A), (B), (C), (D).

Si l'on désigne maintenant par

$$(S) \quad \left\{ \begin{array}{l} (0,0) \ (0,1) \ (0,2) \ (0,3) \\ (1,0) \ (1,1) \ (1,2) \ (1,3) \\ (2,0) \ (2,1) \ (2,2) \ (2,3) \\ (3,0) \ (3,1) \ (3,2) \ (3,3) \end{array} \right.$$

combien des nombres

$$\begin{aligned} &1 + \alpha, 1 + \alpha', 1 + \alpha'', \dots \\ &1 + \beta, 1 + \beta', 1 + \beta'', \dots \\ &1 + \gamma, 1 + \gamma', 1 + \gamma'', \dots \\ &1 + \delta, 1 + \delta', 1 + \delta'', \dots \end{aligned}$$

appartiennent à (A), (B), (C), (D), on pourra déterminer les valeurs de tous ces nombres  $(i, k)$  à l'aide des considérations employées par Gauss dans son premier Mémoire.

Dans le cas actuel, on trouve que le tableau (S) a la forme suivante

$$\begin{array}{cccc} k & j & k & l \\ j & l & m & m \\ k & m & k & m \\ l & m & m & j \end{array} \quad \begin{aligned} 8h &= 4n - 3a - 5, \\ 8j &= 4n + a - 2b - 1, \\ 8k &= 4n + a - 1, \\ 8l &= 4n + a + 2b - 1, \\ 8m &= 4n - a + 1. \end{aligned} \quad \left( n = \frac{aa + bb - 1}{\delta} \right).$$

On a maintenant

$$\left(\left(\frac{1+i}{M}\right)\right) = i^{3m+3j} = i^{-m-j} \quad (-m-j = -n + \frac{1}{4}b).$$

Or (mod 4),

$$\frac{a^2-1}{\delta} \equiv \frac{-a+1}{4},$$

$$\frac{b^2}{\delta} \equiv \pm \frac{1}{2}b;$$

onc

$$\begin{aligned} n &\equiv \frac{1}{4}(-a+1+2b), \\ -m-j &= \frac{1}{4}(a-1-b). \end{aligned}$$

Enfin

$$\left(\left(\frac{1+i}{M}\right)\right) = i^{\frac{1}{4}(a-1-b)}.$$

Les autres cas peuvent se traiter d'une manière analogue.

La même méthode réussit pour déterminer le caractère cubique de  $1-\varrho$ , et encore pour trouver les théorèmes sur le nombre 2 dans la théorie des résidus quadratiques. Dans ce dernier cas, après avoir déterminé les nombres  $(i, k)$ , il n'est pas nécessaire de recourir à ces congruences identiques, comme plus haut celle-ci

$$(x-\delta)(x-\delta')(x-\delta'')\dots \equiv x^{\frac{\mu-1}{4}} + i \pmod{M}.$$

Mais on arrive au but par une considération arithmétique, qui ne diffère pas de celle que Gauss a employée dans son premier mémoire pour le nombre 2, dans la théorie des résidus biquadratiques. On a, de cette manière, une démonstration assez simple et purement arithmétique de ces théorèmes

$$\left(\frac{2}{p}\right) = +1, \quad p = 8n \pm 1,$$

$$\left(\frac{2}{p}\right) = -1, \quad p = 8n \pm 3.$$

## XVII.

(Paris, C.-R. Acad. Sci., 96, 1883, 764—766)

---

Sur le nombre des diviseurs d'un nombre entier.

(Note présentée par M. Hermite.)

Désignons par  $f(n)$  le nombre des diviseurs de  $n$ ; nous allons faire voir qu'on a alors

$$(1) \quad \dots \lim_{n=\infty} \left[ \frac{f(1) + f(2) + \dots + f(n)}{n} - \log n \right] = A.$$

$A$  est une constante égale à  $-1 - 2\Gamma'(1)$ ; sa valeur numérique est

$$A = 0,154431329803\dots,$$

Voici quelques valeurs de la fonction qui figure dans le premier membre de la formule (1)

$$\begin{array}{ll} n = 100, & A = 0,2148\dots\dots, \\ n = 1000, & A = 0,161245\dots\dots, \\ n = 100000, & A = 0,154574535\dots\dots \end{array}$$

En considérant l'ensemble des nombres  $1, 2, \dots, n$  avec leurs diviseurs, on voit facilement que le nombre de fois que  $p \leq n$  y figure est  $E\left(\frac{n}{p}\right)$ ; donc

$$f(1) + f(2) + \dots + f(n) = \sum_{p=1}^{p=n} E\left(\frac{n}{p}\right).$$

Nommons  $r_1, r_2, r_3, \dots$  les restes que l'on obtient en divisant  $n$



$$\frac{f(1) + f(2) + \dots + f(n)}{n} - \log n = \sum_1^n \frac{1}{p} - \log n - \sum_1^n \frac{r_p}{n(n-p+1)}$$

Or on sait que

$$\lim_{n=\infty} \sum_1^n \frac{1}{p} - \log n = -\Gamma'(1),$$

et dès lors nous n'aurons plus qu'à démontrer que l'expression

$$(2) \quad \dots \dots \dots \sum_1^n \frac{r_p}{n(n-p+1)}$$

converge vers une limite déterminée.

Or cela est facile, en remarquant que l'on a

$$\lim_{n=\infty} \sum_1^{n-E\left(\frac{n}{2}\right)} \frac{r_p}{n(n-p+1)} = \int_0^{\frac{1}{2}} \frac{x dx}{1-x} = \log 2 - \frac{1}{2},$$

$$\lim_{\substack{n=\infty \\ n-E\left(\frac{n}{2}\right)+1}}^{n-E\left(\frac{n}{3}\right)} \frac{r_p}{n(n-p+1)} = \int_0^{\frac{1}{3}} \frac{x dx}{1-x} = \log \frac{3}{2} - \frac{1}{3},$$

$$\lim_{\substack{n=\infty \\ n-E\left(\frac{n}{3}\right)+1}}^{n-E\left(\frac{n}{4}\right)} \frac{r_p}{n(n-p+1)} = \int_0^{\frac{1}{4}} \frac{x dx}{1-x} = \log \frac{4}{3} - \frac{1}{4},$$

en sorte que l'on obtient pour la limite de l'expression (2)

$$\sum_1^\infty \left[ \log \left( \frac{p+1}{p} \right) - \frac{1}{p+1} \right] = \sum_1^\infty \left[ \frac{1}{2} \left( \frac{1}{p+1} \right)^2 + \frac{1}{3} \left( \frac{1}{p+1} \right)^3 + \frac{1}{4} \left( \frac{1}{p+1} \right)^4 + \dots \right]$$

ou bien, en posant  $S_k = \sum_1^\infty \frac{1}{p^k}$ ,

$$(3) \quad \lim_{n=\infty} \sum_1^n \frac{r_p}{n(n-p+1)} = \frac{1}{2} (S_2 - 1) + \frac{1}{3} (S_3 - 1) + \frac{1}{4} (S_4 - 1) + \dots$$

Maintenant, on considère le développement

$$\log \Gamma(1-x) = -\Gamma'(1)x + \frac{1}{2} S_2 x^2 + \frac{1}{6} S_3 x^3 + \frac{1}{24} S_4 x^4 + \dots;$$

en retranchant

$$\log \frac{1}{1-x} = x + \frac{1}{2} x^2 + \frac{1}{3} x^3 + \dots,$$

on aura

$$\log \Gamma(2-x) = -[1 + \Gamma'(1)]x + \frac{1}{2}(S_2-1)x^2 + \frac{1}{3}(S_3-1)x^3 + \dots$$

et, posant  $x=1$ ,

$$1 + \Gamma'(1) = \frac{1}{2}(S_2-1) + \frac{1}{3}(S_3-1) + \dots;$$

donc

$$(4) \quad . . . . . \lim_{n \rightarrow \infty} \sum_1^n \frac{r_p}{n(n-p+1)} = 1 + \Gamma'(1),$$

ce qui achève la démonstration du résultat annoncé.

---

## XVIII.

(Paris, C.-R. Acad. Sci., 97, 1883, 740—742.)

---

### Sur l'évaluation approchée des intégrales.

(Note présentée par M. Hermite.)

Soit  $f(x)$  une fonction qui reste constamment positive quand la variable croît de  $x=a$  jusqu'à  $x=b$ , et considérons l'intégrale

$$1) \quad \dots \int_a^b f(x) \mathfrak{F}(x) dx.$$

M. Heine, dans son beau *Traité des fonctions sphériques*, a démontré que, si  $\mathfrak{F}(x)$  est un polynôme du degré  $2n-1$  au plus, la valeur de cette intégrale peut s'obtenir à l'aide de  $n$  valeurs spéciales convenablement choisies,  $\mathfrak{F}(x_1), \mathfrak{F}(x_2), \dots, \mathfrak{F}(x_n)$ . Les valeurs  $x_1, x_2, \dots, x_n$  sont toutes différentes entre elles et s'obtiennent comme les racines d'une équation du degré  $n$ ,

$$\mathfrak{N}(x) = x^n + a_1 x^{n-1} + \dots = 0,$$

dont les coefficients dépendent des  $2n$  constantes

$$c_t = \int_a^b x^t f(x) dx.$$

$$(t=0, 1, 2, \dots, 2n-1)$$

La valeur de l'intégrale (1) se présente alors sous la forme

$$A_1 \mathfrak{F}(x_1) + A_2 \mathfrak{F}(x_2) + \dots + A_n \mathfrak{F}(x_n).$$

$$(2) \quad \dots \int_a^b f(x) \frac{\mathfrak{U}(x)}{x - x_k} dx = \mathfrak{U}'(x_k) A_k,$$

$$(3) \quad \dots \int_a^b f(x) \left[ \frac{\mathfrak{U}(x)}{x - x_k} \right]^2 dx = [\mathfrak{U}'(x_k)]^2 A_k,$$

$$(4) \quad \dots \int_a^b x^t f(x) \mathfrak{U}(x) dx = 0.$$

$$(t = 0, 1, 2, \dots, n-1)$$

La formule (3) fait voir que les coefficients  $A_1, A_2, \dots, A_n$ , sont tous positifs.

Soit maintenant  $\mathfrak{G}(x)$  une fonction qui reste continue et ne présente qu'un nombre fini de maxima et minima entre les limites  $x=a, x=b$ . On a, dans cette supposition, le développement en série

$$\mathfrak{G}(x) = \sum_0^{\infty} a_k X_k \left( \frac{2x - a - b}{b - a} \right),$$

$X_k$  étant le polynôme connu de Legendre. Cette série, d'après ce qu'a démontré M. Heine, est convergente uniformément pour toutes les valeurs de  $x$  entre  $a$  et  $b$ . Il s'ensuit qu'en posant

$$\mathfrak{F}(x) = \sum_0^{2n-1} a_k X_k \left( \frac{2x - a - b}{b - a} \right),$$

$$\mathfrak{R}(x) = \sum_{2n}^{\infty} a_k X_k \left( \frac{2x - a - b}{b - a} \right),$$

on pourra prendre  $n$  toujours assez grand, pour que  $\mathfrak{R}(x)$  reste constamment inférieur en valeur absolue à une quantité arbitraire  $\varepsilon$ .

Or on a

$$\mathfrak{G}(x) = \mathfrak{F}(x) + \mathfrak{R}(x),$$

donc

$$\begin{aligned} \int_a^b f(x) \mathfrak{G}(x) dx - \sum_1^n A_k \mathfrak{G}(x_k) &= \int_a^b f(x) \mathfrak{F}(x) dx - \sum_1^n A_k \mathfrak{F}(x_k) + \\ &+ \int_a^b f(x) \mathfrak{R}(x) dx - \sum_1^n A_k \mathfrak{R}(x_k). \end{aligned}$$

Mais,  $\mathfrak{F}(x)$  étant un polynôme du degré  $2n-1$ , on a

$$\int_a^b f(x) \mathfrak{F}(x) dx - \sum_1^n A_k \mathfrak{F}(x_k) = 0.$$

De plus, les nombres  $A_1, A_2, \dots, A_n$  étant positifs et leur somme égale à  $\int_a^b f(x) dx$ , on a

$$\sum_1^n A_k \mathfrak{R}(x_k) < \varepsilon \int_a^b f(x) dx;$$

de même,

$$\int_a^b f(x) \mathfrak{R}(x) dx < \varepsilon \int_a^b f(x) dx.$$

On en conclut que la différence

$$\int_a^b f(x) \mathfrak{G}(x) dx - \sum_1^n A_k \mathfrak{G}(x_k)$$

est inférieure à  $2\varepsilon \int_a^b f(x) dx$ . En prenant donc  $\sum_1^n A_k \mathfrak{G}(x_k)$  pour valeur approchée de  $\int_a^b f(x) \mathfrak{G}(x) dx$ , l'erreur peut devenir aussi petite qu'on veut par une détermination convenable du nombre  $n$ .

---

## XIX.

(Paris, C.-R. Acad. Sci., 97, 1883, 798—799.)

---

### Sur l'évaluation approchée des intégrales.

(Note présentée par M. Hermite.)

Voici encore quelques autres circonstances qui se rattachent à la remarque que  $A_k$  est positif. Considérons l'expression

$$\Omega = \int_a^b \frac{f(z)}{x-z} dz = \frac{c_0}{x} + \frac{c_1}{x^2} + \frac{c_2}{x^3} + \dots$$

On sait que le polynôme  $\mathfrak{N}(x)$  qui détermine les valeurs  $\dots, x_n$  est le dénominateur de la réduite d'ordre  $n$  de la fraction continue

$$(5) \quad \Omega = \frac{c_0}{x - a_0 - \frac{\lambda_1}{x - a_1 - \frac{\lambda_2}{x - a_2 - \frac{\lambda_3}{x - a_3 - \dots}}}}$$

Posons

$$\begin{array}{ll} P_0 = 0, & Q_0 = 1, \\ P_1 = c_0, & Q_1 = x - a_0, \\ P_2 = (x - a_1) P_1 - \lambda_1 P_0, & Q_2 = (x - a_1) Q_1 - \lambda_1 Q_0, \\ P_3 = (x - a_2) P_2 - \lambda_2 P_1, & Q_3 = (x - a_2) Q_2 - \lambda_2 Q_1, \\ \dots & \dots \end{array}$$

alors  $\mathfrak{N}(x) = Q_n$  et

En faisant attention aux équations (4), cette dernière formule fait bien voir que le développement de  $Q_n \Omega - P_n$  suivant les puissances descendantes de  $x$  commence par un terme en  $x^{-n-1}$ .

La comparaison de (2) et (6) donne

$$Q'_n(x_k) A_k = P_n(x_k).$$

Si l'on suppose  $x_1 > x_2 > x_3 \dots$ , les valeurs  $Q'_n(x_1), Q'_n(x_2), \dots$  seront alternativement positives et négatives.  $A_k$  étant positif, il s'ensuit que de même  $P_n(x_1), P_n(x_2), \dots$  seront alternativement positifs et négatifs. Donc les racines de l'équation

$$P_n(x) = 0$$

séparent celles de l'équation

$$Q_n(x) = 0.$$

En posant  $x = x_1, x = x_2, \dots$  dans la relation connue

$$P_n(x) Q_{n-1}(x) - P_{n-1}(x) Q_n(x) = c_0 \lambda_1 \lambda_2 \dots \lambda_{n-1},$$

on verra facilement que, de même, les racines de  $Q_{n-1}(x) = 0$  séparent celles de  $Q_n(x) = 0$  et, de plus, que  $c_0 \lambda_1 \lambda_2 \dots \lambda_{n-1}$  est positif. Cette conclusion subsistant pour toutes les valeurs de  $n$ , on voit que  $\lambda_1, \lambda_2, \lambda_3, \dots$  sont tous positifs.

Considérons encore la relation

$$Q_n = (x - a_{n-1}) Q_{n-1} - \lambda_{n-1} Q_{n-2},$$

d'où

$$0 = (x_1 - a_{n-1}) Q_{n-1}(x_1) - \lambda_{n-1} Q_{n-2}(x_1),$$

$$0 = (x_n - a_{n-1}) Q_{n-1}(x_n) - \lambda_{n-1} Q_{n-2}(x_n).$$

On voit facilement que  $Q_{n-1}(x_1)$  et  $Q_{n-2}(x_1)$  sont positifs, tandis que  $Q_{n-1}(x_n)$  et  $Q_{n-2}(x_n)$  sont de signes contraires. Il s'ensuit que  $a_{n-1}$  est compris entre  $x_1$  et  $x_n$ .

En somme, nous pouvons affirmer que dans le développement en fraction continue (5),  $\lambda_1, \lambda_2, \lambda_3, \dots$  sont tous positifs, tandis que  $a_0, a_1, a_2, \dots$  ont des valeurs comprises entre  $a$  et  $b$ .

## XX.

(Paris, C.-R. Acad. Sci., 97, 1883, 889—892.)

---

### Sur quelques théorèmes arithmétiques.

(Extrait d'une lettre adressée à M. Hermite.)

Soit  $f(n)$  le nombre des solutions de l'équation

$$n = x^2 + y^2;$$

lorsque  $n$  est impair on a, comme on sait,

$$f(2n) = f(n);$$

cela étant, vous trouvez, pour  $n = 4t + 1$ ,

$$\begin{aligned} & f(2.1) + f(2.5) + \dots + (2.n) \\ &= 8 \left[ E\left(\frac{n-1}{4}\right) - E\left(\frac{n-3^2}{3.4}\right) + E\left(\frac{n-5^2}{5.4}\right) - \dots \right] + 4 \cos^2 \frac{(\mu-1)\pi}{4} \end{aligned}$$

$\mu$  étant l'entier impair immédiatement au dessous de  $\sqrt{n}$  ou égal à  $\sqrt{n}$

On a aussi, en supposant  $n = 8t + 1$ ,

$$\begin{aligned} & f(1) + f(9) + f(17) + \dots + f(n) \\ &= 8 \left[ E\left(\frac{n-1}{8}\right) - E\left(\frac{n-3^2}{3.8}\right) + E\left(\frac{n-5^2}{5.8}\right) - \dots \right] + 4 \cos^2 \frac{(\mu-1)\pi}{4} \end{aligned}$$

$\mu$  étant l'entier impair immédiatement au-dessous de  $\sqrt{n}$  ou égal à  $\sqrt{n}$

et encore, pour  $n = 8t + 5$ ,

$$\begin{aligned} & f(5) + f(13) + f(21) + \dots + f(n) \\ &= 8 \left[ E\left(\frac{n-1.5}{8}\right) - E\left(\frac{n-3.7}{3.8}\right) + E\left(\frac{n-5.9}{5.8}\right) - \dots \right] + \sin^2 \frac{k\pi}{2} \end{aligned}$$



Soit en second lieu  $\varphi(x)$  la somme des diviseurs impairs de  $x$ , y est

$$\begin{aligned} & \varphi(1) + \varphi(5) + \dots + \varphi(4n+1) \\ &= 2 \sum \mathbb{E}^2 \left( \frac{n-k^2+k+1}{2k+1} \right) + 4 \sum k \mathbb{E} \left( \frac{n-k^2+k+1}{2k+1} \right) - \lambda^2, \end{aligned}$$

où

$$\lambda = \mathbb{E} \left( \frac{\sqrt{4n+1}+1}{2} \right).$$

$$(k=0, 1, 2, 3, \dots)$$

En écrivant ceci, je crois voir que cette formule rentrera dans vôtre à l'aide de la relation

$$\mathbb{E}^2 \left( \frac{n-k^2+k+1}{2k+1} \right) + 2k \mathbb{E} \left( \frac{n-k^2+k+1}{2k+1} \right) = \mathbb{E}^2 \left( \frac{n+k^2+2k+1}{2k+1} \right) -$$

On peut écrire encore

$$\begin{aligned} & \varphi(1) + \varphi(5) + \dots + \varphi(n) \\ &= 2 \sum \mathbb{E}^2 \left( \frac{n-r^2}{4r} \right) + 4 \sum \frac{r+1}{2} \mathbb{E} \left( \frac{n-r^2}{4r} \right) + \mathbb{E}^2 \left( \frac{\sqrt{n}+1}{2} \right). \end{aligned}$$

$$(r=1, 3, 5, 7, \dots)$$

J'obtiens encore

$$\begin{aligned} & \varphi(1) + \varphi(3) + \varphi(5) + \dots + \varphi(2n-1) \\ &= \sum \mathbb{E}^2 \left( \frac{n-2k^2}{2k+1} \right) + \sum (4k+1) \mathbb{E} \left( \frac{n-2k^2}{2k+1} \right) - \mathbb{E}^2 \left( \frac{\sqrt{2n-1}+1}{2} \right). \end{aligned}$$

$$(k=0, 1, 2, 3, \dots)$$

On a enfin

$$\varphi(1) + \varphi(2) + \dots + \varphi(n) = \mathbb{E} \left( \frac{n}{1} \right) + 3 \mathbb{E} \left( \frac{n}{3} \right) + 5 \mathbb{E} \left( \frac{n}{5} \right) + \dots,$$

puis, au moyen d'une transformation analogue à celle que vous avez faite de la somme

$$\mathbb{E} \left( \frac{n}{1} \right) - \mathbb{E} \left( \frac{n}{3} \right) + \dots,$$

on trouve

$$\varphi(1) + \varphi(2) + \dots + \varphi(n) = S + S_1 - \lambda^3$$

en posant

$$S = \mathbb{E} \left( \frac{n}{1} \right) + 3 \mathbb{E} \left( \frac{n}{3} \right) + \dots + (2\lambda-1) \mathbb{E} \left( \frac{n}{2\lambda-1} \right),$$

$$S_1 = \mathbb{E}^2 \left( \frac{n+1}{2} \right) + \mathbb{E}^2 \left( \frac{n+2}{4} \right) + \dots + \mathbb{E}^2 \left( \frac{n+\lambda}{2\lambda} \right),$$

$$\lambda = \mathbb{E} \left( \frac{\sqrt{8n+1}+1}{4} \right).$$

Je me suis aussi occupé de la fonction  $F(n)$ , exprimant le nombre des représentations de  $n$ , par la forme  $x^2 + 2y^2$ . La considération de la série

$$\sum_{-\infty}^{+\infty} k \sum_{-\infty}^{+\infty} i q^{k^2 + 2i^2}$$

donne d'abord la formule

$$F(n) = 2(d_1 + d_3 - d_5 - d_7),$$

où  $d_1, d_3, d_5, d_7$  signifient les nombres des diviseurs de  $n$  qui sont compris dans les formes

$$8k + 1, \quad 8k + 3, \quad 8k + 5, \quad 8k + 7,$$

et l'on en conclut

$$F(1) + F(2) + \dots + F(n) = 2 \left[ E\left(\frac{n}{1}\right) + E\left(\frac{n}{3}\right) - E\left(\frac{n}{5}\right) - E\left(\frac{n}{7}\right) + \dots \right].$$

Cela posé, j'obtiens, par une transformation analogue à la vôtre, la formule suivante. Soit, pour abrégér,

$$\varphi(x) = 2 \sin^2 \frac{\pi x}{4},$$

de sorte qu'on ait

$$\varphi(4k + 1) = 1,$$

$$\varphi(4k + 2) = 2,$$

$$\varphi(4k + 3) = 1,$$

$$\varphi(4k) = 0,$$

puis,

$$\lambda = E\left(\frac{\sqrt{8n+1} + 1}{4}\right).$$

et posons

$$S = E\left(\frac{n}{1}\right) + E\left(\frac{n}{3}\right) - E\left(\frac{n}{5}\right) - E\left(\frac{n}{7}\right) + \dots \pm E\left(\frac{n}{2\lambda - 1}\right),$$

$$S_1 = \varphi\left[E\left(\frac{n+1}{2}\right)\right] + \varphi\left[E\left(\frac{n+2}{4}\right)\right] + \dots + \varphi\left[E\left(\frac{n+\lambda}{2\lambda}\right)\right],$$

nous aurons

$$F(1) + F(2) + \dots + F(n) = 2[S + S_1 - \lambda \varphi(\lambda)].$$

## XXI.

(Paris, C.-R. Acad. Sci., 97, 1883, 981—982.)

---

Sur la décomposition d'un nombre en cinq carrés.

(Extrait d'une lettre adressée à M. Hermite.)

Permettez moi de vous communiquer un résultat que je crois nouveau, sur la décomposition d'un nombre  $N \equiv 5, \text{ mod } 8$ , en cinq carrés impairs et positifs. En désignant par  $\varphi(m)$  la somme des diviseurs de  $m$ , le nombre de ces décompositions est

$$\varphi\left(\frac{N-1^2}{4}\right) + \varphi\left(\frac{N-3^2}{4}\right) + \varphi\left(\frac{N-5^2}{4}\right) + \dots$$

C'est une conséquence facile du théorème de Jacobi concernant la décomposition en quatre carrés impairs et positifs d'un nombre  $N \equiv 4, \text{ mod } 8$ ; théorème qu'on peut maintenant considérer comme élémentaire. Or je trouve que ce même nombre des représentations de  $N \equiv 5, \text{ mod } 8$ , par cinq carrés peut s'exprimer aussi par cette nouvelle formule

$$f(N) + 2f(N-8 \cdot 1^2) + 2f(N-8 \cdot 2^2) + 2f(N-8 \cdot 3^2) + \dots$$

La fonction  $f(m)$  est définie de la manière suivante :

$$4f(m) = -\sum (-1)^{\frac{d^2-1}{8}} d,$$

impairs; mais je ne sais si ce théorème peut aussi se tirer de la théorie des fonctions elliptiques<sup>1)</sup>.

<sup>1)</sup> Voici, pour la décomposition en cinq carrés impairs et positifs, une proposition qui donne les formules de la théorie des fonctions elliptiques. Soit  $n$  un entier  $\equiv 1, \text{ mod } 4$ . Posons, de toutes les manières possibles,  $n = d d'$  sous la condition  $d' > 3d$ ; je considérerai la fonction

$$\chi(n) = \Sigma \frac{1}{2} (3d + d'),$$

qui peut être définie par développement

$$\begin{aligned} & \chi(5)q + \chi(9)q^2 + \dots + \chi(4m+1)q^m + \dots \\ &= \frac{q}{1-q} + \frac{4q^8}{1-q^3} + \frac{7q^{21}}{1-q^5} + \dots + \frac{(3m-2)q^{m(3m-2)}}{1-q^{2m-1}} + \dots \\ &+ \frac{q}{(1-q)^2} + \frac{q^8}{(1-q^3)^2} + \frac{q^{21}}{(1-q^5)^2} + \dots + \frac{q^{m(3m-2)}}{(1-q^{2m-1})^2} + \dots \end{aligned}$$

Cela étant, le nombre des décompositions d'un entier  $N \equiv 5, \text{ mod } 8$ , s'obtient par la formule

$$\frac{1}{2} \chi(N) + \chi(N-2^2) + \chi(N-4^2) + \chi(N-6^2) + \dots$$

Supposons, par exemple,  $N = 45$ , ce qui donne

$$\frac{1}{2} \chi(45) = 9, \quad \chi(41) = 11, \quad \chi(29) = 8, \quad \chi(9) = 3;$$

nous aurons 31 pour le nombre cherché, et c'est bien en effet ce qu'on trouve par le développement

$$(\sqrt[4]{q} + \sqrt[4]{q^9} + \sqrt[4]{q^{25}} + \dots)^5 = q^{\frac{5}{4}} (1 + 5q^2 + 10q^4 + 15q^6 + 25q^8 + 31q^{10} + \dots).$$

(C. H.)

## XXII.

(Paris, C.-R. Acad. Sci., 97, 1883, 1358—1359.)

---

### Sur un théorème de Liouville.

(Note, présentée par M. Hermite.)

Dans le Tome XIV (2<sup>e</sup> série, année 1869, p. 1) du Journal de Mathématiques pures et appliquées, Liouville, dans une Lettre adressée à M. Besge, a donné une relation remarquable entre les nombres de classes de formes quadratiques

A l'aide de considérations arithmétiques, j'ai pu établir d'autres relations d'une forme analogue, et je me suis aperçu après qu'on peut établir aussi toutes ces formules à l'aide de la théorie des fonctions elliptiques. Les théorèmes I—IV qui vont suivre sont ceux que je connais jusqu'à présent; le premier théorème est celui qui a été donné par Liouville.

Comme je l'ai déjà dit, on peut vérifier ces théorèmes à l'aide de formules tirées de la théorie des fonctions elliptiques; mais déjà dans le cas du théorème IV, cette vérification demande des calculs assez prolixes.

Désignons généralement par  $F(n)$  le nombre des classes de formes quadratiques de déterminant  $-n$ , dont un au moins des coefficients extrêmes est impair. Toutefois, lorsque  $n$  est un carré impair, il faudra diminuer de  $\frac{1}{2}$  le nombre de ces classes pour avoir  $F(n)$ ; ainsi  $F(1) = \frac{1}{2}$ ,  $F(9) = 2\frac{1}{2}$ , ... Cette convention, qui simplifie les formules a été introduite par M. Kronecker

Cela posé, on a les théorèmes suivants :

Théorème I. — Soit  $N$  un nombre positif impair ; alors

$$\Sigma (-1)^{\frac{s-1}{2}} s F(4N - s^2) = \Sigma (x^2 - y^2)$$

La sommation, dans le second membre, a rapport à toutes les solutions de  $N = x^2 + y^2$ ,  $x$  étant impair et positif,  $y$  étant quelconque positif, nul ou négatif

Théorème II. — Soit  $N$  un nombre positif quelconque ; alors

$$2 \Sigma (-1)^{\frac{s-1}{2}} s F(4N - 2s^2) = (-1)^{\frac{N(N-1)}{2}} \Sigma (x^2 - 2y^2).$$

La sommation, dans le second membre, a rapport à toutes les solutions de  $N = x^2 + 2y^2$ ,  $x$  et  $y$  étant des nombres entiers quelconques, positifs, nuls ou négatifs

Théorème III. — Soit  $N$  un nombre positif de la forme  $8k + 3$  ; alors

$$2 \Sigma (-1)^{\frac{s-1}{2} + \frac{s^2-1}{8}} s F\left(\frac{N-s^2}{2}\right) = (-1)^{\frac{N+5}{8}} \Sigma (x^2 - 2y^2).$$

La sommation, dans le second membre, a rapport à toutes les solutions de  $N = x^2 + 2y^2$ ,  $x$  et  $y$  étant positifs et impairs.

Théorème IV. — Soit  $N$  un nombre positif quelconque ; alors

$$\Sigma (-1)^{\frac{s-1}{2}} s F(16N - 3s^2) = \Sigma (x^2 - 3y^2).$$

La sommation, dans le second membre, a rapport à toutes les solutions de  $N = x^2 + 3y^2$ ,  $x$  et  $y$  étant des nombres entiers quelconques, positifs, nuls ou négatifs, soumis seulement à cette restriction que  $x + y$  doit être impair.

Nous devons ajouter que, dans toutes ces formules, le second membre devient égal à zéro lorsqu'il n'y a pas de représentation de  $N$  par la forme quadratique indiquée. Cela a lieu, par exemple, dans le premier théorème, lorsque  $N$  est de la forme  $4k + 3$ , et dans le quatrième, lorsque  $N$  est pair.

## XXIII.

(Paris, C.-R. Acad. Sci., 97, 1883, 1415—1418.)

---

### Sur un théorème de M. Liouville.

(Note, présentée par M. Hermite.)

Je propose de montrer comment la théorie des fonctions elliptiques conduit au théorème de M. Liouville, qui a été l'objet de ma présente Note.

Désignant par  $K$  et  $E$  les intégrales complètes de première et de seconde espèce, les formules relatives au développement des fonctions de seconde espèce donnent

$$\frac{K(K-E)}{\pi^2} = 2 \frac{q - 4q^4 + 9q^9 - 16q^{16} + 25q^{25} - \dots}{1 - 2q + 2q^4 - 2q^9 + \dots},$$

$$\dots \quad \frac{4KE}{\pi^2} = 2 \frac{q^{\frac{1}{4}} + 9q^{\frac{9}{4}} + 25q^{\frac{25}{4}} + \dots}{q^{\frac{1}{4}} + q^{\frac{9}{4}} + q^{\frac{25}{4}} + \dots}.$$

En remplaçant  $q$  par  $q^4$  dans cette dernière équation, on trouvera

$$\Sigma x^2 q^{x^2} = \frac{K}{\pi^2} \sqrt{\frac{K}{2\pi}} \left[ \frac{1 - \sqrt{k'}}{2} E + \frac{\sqrt{k'}(1 - k' \sqrt{k'})}{2} K \right].$$

( $x = 1, 3, 5, 7, \dots$ )

En appliquant cette formule avec (1), on aura

$$\Sigma y^2 q^{y^2} = \frac{K}{\pi^2} \sqrt{\frac{K}{2\pi}} [(1 + \sqrt{k'}) E - \sqrt{k'}(1 + k' \sqrt{k'}) K],$$

( $y = 0, \pm 2, \pm 4, \pm 6, \dots$ )

$$(y = 0, \pm 2, \pm 4, \dots)$$

Les formules (3), (4), (5), (6) donnent maintenant

$$\Sigma \Sigma (x^2 - y^2) q^{x^2 + y^2} = \frac{K^3}{2 \pi^3} k^2 \sqrt{k'}$$

ou bien

$$(7) \quad 16 \Sigma \Sigma (x^2 - y^2) q^{x^2 + y^2} = \frac{8 K^3}{\pi^3} k^2 \sqrt{k'} = \theta(q) \theta_2^4(q) \theta_3(q),$$

en posant

$$\theta(q) = 1 - 2q + 2q^4 - 2q^9 + \dots = \sqrt{\frac{2k'K}{\pi}},$$

$$\theta_2(q) = 2q^{\frac{1}{4}} + 2q^{\frac{9}{4}} + \dots = \sqrt{\frac{2kK}{\pi}},$$

$$\theta_3(q) = 1 + 2q + 2q^4 + 2q^9 + \dots = \sqrt{\frac{2K}{\pi}}.$$

Or on connaît ce développement

$$\theta(q) \theta_2(q) \theta_3(q) = 2 \left( q^{\frac{1}{4}} - 3q^{\frac{9}{4}} + 5q^{\frac{25}{4}} - \dots \right),$$

et, d'après une formule due à M. Hermite,

$$\theta_2^3(q) = 8 \sum_{n=0}^{\infty} F(8n+3) q^{\frac{8n+3}{4}}.$$

L'équation (7) peut donc s'écrire sous la forme suivante

$$\Sigma (-1)^{\frac{x-1}{2}} x q^{\frac{x^2}{4}} \sum_{n=0}^{\infty} F(8n+3) q^{\frac{8n+3}{4}} = \Sigma \Sigma (x^2 - y^2) q^{x^2 + y^2}$$

où il faut poser  $x = 1, 3, 5, 7, \dots$  et  $y = 0, \pm 2, \pm 4, \dots$

Cette formule donne immédiatement le théorème de M. Liouville en comparant dans les deux membres les coefficients des puissances de  $q$ .

Remarquons que les relations connues

$$\theta(q) \theta_3(q) = \theta^2(q^2) \quad \text{et} \quad \theta_2^2(q) = 2 \theta_2(q^2) \theta_3(q^2)$$

donnent

$$\theta(q) \theta_2^4(q) \theta_3(q) = 4 [\theta(q^2) \theta_2(q^2) \theta_3(q^2)]^2 = 16 \left[ \Sigma (-1)^{\frac{x-1}{2}} x q^{\frac{x^2}{2}} \right]^2$$



On aurait donc pu établir la formule (7) un peu plus simplement en formant directement le carré de cette série  $\sum_{s=0}^{s-1} (-1)^{\frac{s-1}{2}} x y^2$ ; mais les formules (3) et (4), dont nous nous sommes servi, peuvent être utiles dans d'autres cas.

Ajoutons encore aux théorèmes déjà énoncés les trois suivants.

**Théorème V.** — Soit  $N$  un nombre positif de la forme  $8k + 9$ ; alors

$$8 \sum_{s=0}^{s-1} (-1)^{\frac{s-1}{2}} s F(N - 2s^2) = \sum (x^2 - y^2).$$

La sommation, dans le second membre, a rapport à toutes les solutions de l'équation  $2N = x^2 + y^2$ ,  $x^2$  étant un carré de la forme  $8k + 9$  et, par suite,  $y^2$  un carré de la forme  $8k + 1$ .

**Théorème VI.** — Soit  $N$  un nombre positif de la forme  $8k + 1$ ; alors

$$2 \sum_{s=0}^{s-1} (-1)^{\frac{s-1}{2} + \frac{s^2-1}{8}} s F(2N - s^2) = \sum (-1)^{\frac{s-1}{2}} (x^2 - 8y^2).$$

La sommation, dans le second membre, doit s'étendre à toutes les solutions de l'équation  $N = x^2 + 8y^2$ ,  $x$  étant positif et impair,  $y$  un nombre quelconque, positif, nul ou négatif.

**Théorème VII.** — Soit  $N$  un nombre de la forme  $8k + 5$ ; alors

$$2 \sum_{s=0}^{s-1} (-1)^{\frac{s-1}{2} + \frac{s^2-1}{8}} s F(2N - s^2) = \sum (x^2 - y^2).$$

La sommation, dans le second membre, doit s'étendre à toutes les solutions de l'équation  $2N = x^2 + y^2$ ,  $x^2$  étant un carré de la forme  $8k + 5$ ,  $y^2$  un carré de la forme  $8k + 1$ .

Dans ces formules, le second membre devient égal à zéro toutes les fois qu'il n'y a pas de représentation de  $2N$  ou de  $N$  par la forme indiquée.

## XXIV.

(Paris, C.-R. Acad. Sci., 97, 1883, 1545—1547.)

---

Sur le nombre de décompositions d'un entier en cinq carrés

(Extrait d'une lettre adressée à M. Hermite.)

Dans votre dernière lettre vous m'avez communiqué ces deux formules

$$\begin{aligned}
 (a) \quad & \left\{ \begin{aligned} & q + 4q^4 + 9q^9 + 16q^{16} + \dots \\ & = (1 + 2q + 2q^4 + 2q^9 + \dots) \left[ \frac{q}{(1+q)^2} + \frac{q^8}{(1+q^3)^2} + \frac{q^5}{(1+q^5)^2} + \dots \right] \end{aligned} \right. \\
 (b) \quad & \left\{ \begin{aligned} & q^{\frac{1}{4}} + 9q^{\frac{9}{4}} + 25q^{\frac{25}{4}} + \dots \\ & = (q^{\frac{1}{4}} + q^{\frac{9}{4}} + q^{\frac{25}{4}} + \dots) \left[ 1 + \frac{8q^2}{(1+q^2)^2} + \frac{8q^4}{(1+q^4)^2} + \frac{8q^6}{(1+q^6)^2} + \dots \right] \end{aligned} \right.
 \end{aligned}$$

C'est en étudiant votre première formule (a) que j'ai été amené à considérer de nouveau cette fonction  $F(n)$  qui représente le nombre total des solutions de  $n = x^2 + y^2 + z^2 + t^2 + u^2$ .

Le nombre des solutions de  $n = x^2 + y^2 + z^2 + t^2$  étant

$$8 [2 + (-1)^n] \varphi(n),$$

$\varphi(n)$  désignant la somme des diviseurs impairs de  $n$ , il s'ensuit

$$\begin{aligned}
 F(n) = & 16 [\varphi(n) + 2\varphi(n-1) + 2\varphi(n-4) + 2\varphi(n-9) + \dots] \\
 & + 8(-1)^n [\varphi(n) - 2\varphi(n-1) + 2\varphi(n-4) - 2\varphi(n-9) + \dots]
 \end{aligned}$$

Il est essentiel d'observer que, lorsque  $n$  est un carré, il faut en

s aurons donc

$$\begin{cases} F(n) = 24 A(n) + 16 B(n) & (n \text{ pair}), \\ F(n) = 8 A(n) + 48 B(n) & (n \text{ impair}). \end{cases}$$

Maintenant votre formule (a) donne aisément les relations suivantes

$$A(n) = 4 B(n) \quad (n \equiv 3, \text{ mod } 4),$$

$$A(n) = 8 B(n) \quad (n \equiv 5, \text{ mod } 8),$$

$$A(n) = B(n) \quad (n \equiv 2, \text{ mod } 4).$$

Il s'ensuit donc une simplification de l'expression de  $F(n)$  dans les formules (2). Or je trouve qu'une telle réduction est toujours possible. On peut, en effet, exprimer toujours ces deux fonctions  $A(n)$ ,  $B(n)$  l'une par l'autre. Voici, à cet effet, les formules

$$A(n) = 4 B(n) \quad (n \equiv 3, \text{ mod } 4),$$

$$A(n) = 24 B(n) \quad (n \equiv 1, \text{ mod } 8),$$

$$A(n) = 8 B(n) \quad (n \equiv 5, \text{ mod } 8),$$

$$8^k A(n) = \frac{2^{3k+1} + 5}{7} B(n) \quad (n = 2^{2k+1} m, m \equiv 1, \text{ mod } 2, k = 0, 1, 2, 3, \dots),$$

$$8^k A(n) = \frac{2^{3k+1} + 5}{7} B(n) \quad (n = 4^k m, m \equiv 3, \text{ mod } 4, k = 1, 2, 3, \dots),$$

$$6 \cdot 8^k A(n) = \frac{3 \cdot 2^{3k+2} - 5}{7} B(n) \quad (n = 4^k m, m \equiv 1, \text{ mod } 8, k = 1, 2, 3, \dots),$$

$$2 \cdot 8^k A(n) = \frac{2^{3k+2} + 3}{7} B(n) \quad (n = 4^k m, m \equiv 5, \text{ mod } 8, k = 1, 2, 3, \dots).$$

Une réduction ultérieure de l'expression de  $F(n)$  est possible à l'aide de ces relations

$$B(4n) = 16 B(n) \quad (n \equiv 3, \text{ mod } 4),$$

$$B(4n) = 96 B(n) \quad (n \equiv 1, \text{ mod } 8),$$

$$B(4n) = 32 B(n) \quad (n \equiv 5, \text{ mod } 8),$$

$$B(4n) = 8 B(n) \quad (n \text{ pair}).$$

On trouvera de cette manière

$$\begin{cases} F(24^k \cdot m) = 40 f(k) B(2m) & (m \equiv 1, \text{ mod } 2), \\ F(4^k \cdot m) = 80 f(k) B(m) & (m \equiv 3, \text{ mod } 4), \\ F(4^k \cdot m) = 240 [2 f(k) - 1] B(m) & (m \equiv 1, \text{ mod } 8), \\ F(4^k \cdot m) = 16 [10 f(k) - 3] B(m) & (m \equiv 5, \text{ mod } 8), \end{cases}$$

$k = 0, 1, 2, 3, \dots$

où j'ai posé, pour abrégé,

$$f(k) = \frac{2^{3k+2} + 3}{7},$$

donc

$$f(0) = 1, \quad f(1) = 5, \quad f(2) = 37, \quad \dots, \quad f(k+1) = 8f(k) - 3.$$

On voit par conséquent qu'on peut dans tous les cas exprimer  $F(4n)$  par  $F(n)$ .

Ayant construit une table de la fonction  $B(n)$  pour les premières centaines, j'ai observé qu'on a toujours,  $p$  étant un nombre premier impair,

$$B(p^2) = \frac{p^3 - p + 1}{24}.$$

Ayant vérifié cette formule dans un grand nombre de cas, je n'ai pas de doute qu'elle ne soit vraie généralement, quoique je ne l'aie pas encore démontré. On a donc aussi

$$F(p^2) = 10(p^3 - p + 1).$$

Peut-être a-t-on encore

$$B(p^4) = \frac{p(p^2 - 1)(p^3 + 1) + 1}{24}$$

t

$$F(p^4) = 10[p(p^2 - 1)(p^3 + 1) + 1],$$

mais je n'ai vérifié cette relation que pour  $p = 3, 5$  et  $7$  : les calculs deviennent trop laborieux.

---

## XXV.

(Amsterdam, Versl. K. Akad. Wet., 1<sup>o</sup> sect., sér. 2, 19,  
1884, 105—111.)

---

### Over de quadratische ontbinding van priemgetallen van den vorm $3n + 1$ .

Elk priemgetal  $p = 3n + 1$  kan voorgesteld worden als de som  
van eene volkomen tweede macht en het drievoud van eene andere  
volkomen tweede macht

$$p = cc + 3 dd$$

Het viervoud van zulk een priemgetal kan verder steeds aldus  
voorgesteld worden

$$4p = AA + 27 BB$$

Elk dezer ontbindingen is slechts op ééne wijze mogelijk. Dit  
resultaat valt gemakkelijk uit de algemeene theorie der quadratische  
vormen af te leiden.

In het tweede deel van Crelle's Journal heeft Jacobi, in de ver-  
handeling „de residuis cubicis commentatio numerosa” zonder bewijs  
aangegeven, dat de waarde van A in (2) gelijk is aan de rest, die  
men verkrijgt bij de deeling van het geheele getal

$$\frac{(n+1)(n+2)(n+3)\dots(2n)}{1.2.3\dots n}$$

voor  $p$ , waarbij men deze rest tusschen  $-\frac{1}{2}p$  en  $+\frac{1}{2}p$  te kiezen  
moet. Hierbij doet zich dan nog de merkwaardige omstandigheid  
voor, dat  $A + 1$ , bij deze bepaling van A, steeds door 3 deelbaar is.

Voor de eerste priemgetallen verkrijgt men bijv.:

$p = 7$	$n = 2$	$A = -1$	$28 = 1^2 + 27.1^2$
$p = 13$	$n = 4$	$A = +5$	$52 = 5^2 + 27.1^2$
$p = 19$	$n = 6$	$A = -7$	$76 = 7^2 + 27.1^2$
$p = 31$	$n = 10$	$A = -4$	$124 = 4^2 + 27.2^2$
$p = 37$	$n = 12$	$A = +11$	$148 = 11^2 + 27.1^2$
$p = 43$	$n = 14$	$A = +8$	$172 = 8^2 + 27.2^2$
$p = 61$	$n = 20$	$A = -1$	$244 = 1^2 + 27.3^2$

Het bewijs van deze eigenschap, die in een nauw verband staat met de eigenschappen der algebraïsche vergelijking, van welke de verdeeling van den cirkelomtrek in  $p$  deelen afhangt, is te vinden in Cauchy's *Mémoire sur la théorie des nombres* (Mém. de l'Acad. d. Sc., t. 17, 1840) en bij Lebesgue in het *Journal de Liouville* t. 2, p. 279. Voor verdere bijzonderheden is te verwijzen naar Bachmann: *Die Lehre von der Kreistheilung*, p. 144.

Op andere wijze is dit theorema van Jacobi ook afgeleid in de verhandeling „Bijdrage tot de theorie der derde- en vierde-machts-resten” in het 17<sup>de</sup> deel der Verslagen en Mededeelingen der Koninklijke Akademie van Wetenschappen en wel aldaar in art 40, p. 416.

Aanknoopende aan de ontwikkelingen daar voorkomende, wensch ik hier, uit het theorema van Jacobi, eene directe bepaling van den wortel  $c$  van het enkelvoudige kwadraat in (1) af te leiden; het zal dan blijken, dat  $c$  de tusschen  $-\frac{1}{2}p$  en  $+\frac{1}{2}p$  gelegen rest is, die men verkrijgt bij de deeling van het geheele getal

$$2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n}$$

door  $p$ , en verder is dan  $c-1$  door 3 deelbaar. Bijv.:

$p = 7$	$n = 2$	$c = -2$	$7 = 2^2 + 3.1^2$
$p = 13$	$n = 4$	$c = +1$	$13 = 1^2 + 3.2^2$
$p = 19$	$n = 6$	$c = +4$	$19 = 4^2 + 3.1^2$
$p = 31$	$n = 10$	$c = -2$	$31 = 2^2 + 3.3^2$
$p = 37$	$n = 12$	$c = -5$	$37 = 5^2 + 3.2^2$

Zij dan, evenals in de aangehaalde verhandeling,  $\varrho$  een primitieve demachtswortel der eenheid,  $a + b\varrho$  een primaire factor van  $p$ , dus

$$p = (a + b\varrho)(a + b\varrho^2) = a^2 - ab + b^2,$$

$a$  en  $b$  beiden door 3 deelbaar; verder  $f$  een der beide wortels van de congruentie:

$$1 + x + x^2 \equiv 0 \pmod{p}$$

wel  $f$  zóó gekozen, dat  $a + bf$  door  $p$  deelbaar is.

Volgens het boven aangehaalde theorema van Jacobi is dan

$$\dots \quad 2a - b \equiv - \frac{(n+1)(n+2)\dots(2n)}{1 \cdot 2 \cdot 3 \dots n} \pmod{p}$$

verder is volgens de criteria voor het cubisch karakter van 2

$$2^n \equiv 1$$

wanneer  $b$  even is,

$$2^n \equiv f \pmod{p}$$

wanneer  $a$  even is,

$$2^n \equiv f^2$$

wanneer  $a$  en  $b$  beiden oneven zijn. (Zie t. a. p. p. 398.)

Deze drie gevallen moeten nu afzonderlijk behandeld worden.

I.  $\dots$   $b$  even.

In dit geval leiden wij uit

$$p = a^2 - ab + b^2$$

$$\begin{aligned} 4p &= (2a - b)^2 + 3b^2 \\ &= (a - \tfrac{1}{2}b)^2 + 3(\tfrac{1}{2}b)^2. \end{aligned}$$

In de vergelijking (1) kan dus genomen worden

$$c = -(a - \tfrac{1}{2}b).$$

Uit (3) volgt dan

$$c \equiv \tfrac{1}{2} \cdot \frac{(n+1)(n+2)\dots(2n)}{1 \cdot 2 \cdot 3 \dots n} \pmod{p}$$

wel, daar in dit geval  $2^n \equiv 1$  is,

$$\dots \quad c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1 \cdot 2 \cdot 3 \dots n} \pmod{p}.$$

Uit  $a \equiv 2, b \equiv 0 \pmod{3}$  volgt verder

$$(5^a) \quad \dots \dots \dots c \equiv 1 \pmod{3}.$$

II.  $a$  even.

In dit geval schrijven wij in plaats van

$$p = a^2 - ab + b^2$$

$$16p = (2a - 4b)^2 + 3(2a)^2$$

of

$$p = \left(\frac{1}{2}a - b\right)^2 + 3\left(\frac{1}{2}a\right)^2,$$

zoodat wij in (1) kunnen nemen

$$c = \frac{1}{2}a - b.$$

Nu is

$$(6) (a + bf)(1 + 2f) \equiv a - 2b + (2a - b)f \equiv -a - b - (2a - b)f^2 \pmod{p}$$

en  $a + bf \equiv 0 \pmod{p}$ , derhalve

$$a - 2b \equiv -f(2a - b),$$

zoodat uit (3) volgt

$$a - 2b \equiv f \frac{(n+1)(n+2)\dots(2n)}{1 \cdot 2 \cdot 3 \dots n}$$

of wel, daar nu  $f \equiv 2^n$  is,

$$(4^b) \quad \dots \dots \dots c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1 \cdot 2 \cdot 3 \dots n} \pmod{p}.$$

Uit  $a \equiv 2, b \equiv 0 \pmod{3}$  volgt verder

$$(5^b) \quad \dots \dots \dots c \equiv 1 \pmod{3}$$

III.  $a$  en  $b$  oneven.

In dit laatste geval bedenke men, dat

$$16p = (2a + 2b)^2 + 3(2a - 2b)^2$$

is, of

$$p = \left(\frac{a+b}{2}\right)^2 + 3\left(\frac{a-b}{2}\right)^2,$$

zoodat genomen kan worden

$$c = \frac{a+b}{2}.$$



at (6) volgt nu  $a + b \equiv -f^2(2a - b)$ , dus geeft (3)

$$a + b \equiv f^2 \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p}.$$

Daar nu in dit geval  $2^n \equiv f^2$  is, zoo volgt

$$\dots\dots\dots c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p},$$

is gemakkelijk te zien is

$$\dots\dots\dots c \equiv 1 \pmod{3}.$$

Uit de vergelijkingen  $4^a, 4^b, 4^c, 5^a, 5^b, 5^c$  blijkt nu, dat men in elk geval heeft

$$\dots\dots\dots c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p}$$

$$\dots\dots\dots c \equiv 1 \pmod{3},$$

Daar dus het boven reeds uitgesproken theorema geeft. De constantie (4) kan men nog een anderen vorm geven. Daar  $n$  even is, schrijve men  $2m$  voor  $n$ , dan is

$$c \equiv 2^{2m-1} \frac{(2m+1)(2m+2)\dots(4m)}{1.2.3\dots(2m)}.$$

Daar nu is

$$\begin{aligned} 2m+1 &\equiv -(4m), & 2m+3 &\equiv -(4m-2), \\ 2m+5 &\equiv -(4m-4) \dots \text{enz.} \end{aligned}$$

kan behulp waarvan men verkrijgt

$$c \equiv (-1)^m 2^{2m-1} \frac{[(2m+2)(2m+4)\dots(4m)]^2}{1.2.3\dots(2m)}.$$

Daar eene kleine herleiding

$$c \equiv (-1)^m 2^{4m-1} \frac{(m+1)(m+2)\dots(2m)}{1.2.3\dots m}.$$

Daar nu is verder

$$2^{8m} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}}$$

$$\frac{p^2-1}{8} = \frac{9m^2+3m}{2}.$$

Van dezen exponent het even getal  $\frac{8m^2 + 4m}{2}$  aftrekkende, kan men eenvoudiger schrijven

$$2^{8m} \equiv (-1)^{\frac{m^2 - m}{2}},$$

dus ten slotte

$$7) \quad c \equiv (-1)^{\frac{m^2 + m}{2}} 2^{m-1} \frac{(m+1)(m+2) \dots (2m)}{1 \cdot 2 \cdot 3 \dots m} \pmod{p = 6m + 1}.$$

Deze laatste congruentie ter bepaling van  $c$  is zonder bewijs, en zonder de hier verkregen nadere bepaling van het teeken van  $c$ , gegeven door Oltramare in het 87<sup>ste</sup> deel der Comptes rendus de l'Acad. d. Sc., p. 735, te gelijk met meer soortgelijke.

## XXV.

(Amsterdam, Versl. K. Akad. Wet., 1<sup>e</sup> sect., sér. 2, 19,  
1884, 105—111.)

---

### Sur la décomposition quadratique de nombres premiers de la forme $3n + 1$ .

Chaque nombre premier  $p = 3n + 1$  peut être représenté par la somme d'un carré parfait et de trois fois un deuxième carré parfait

$$p = cc + 3dd$$

En outre, le quadruple d'un nombre premier de ce genre peut toujours être représenté par l'expression suivante

$$4p = AA + 27BB$$

L'une et l'autre décomposition ne sont possibles que d'une seule manière pour chaque nombre  $p$ . Tout ceci se déduit aisément de la théorie générale des formes quadratiques.

Dans le deuxième tome du Journal de Crelle, Jacobi, dans son mémoire „de residuis cubicis commentatio numerosa” a énoncé, sans donner la démonstration, le théorème suivant: la valeur de  $A$  dans l'expression (2) est égale au résidu qu'on obtient lorsqu'on divise le nombre entier

$$\frac{(n+1)(n+2)(n+3)\dots(2n)}{1.2.3\dots n}$$

par  $p$ ; il est entendu qu'il faut prendre pour résidu un nombre compris entre  $-\frac{1}{2}p$  et  $+\frac{1}{2}p$ . Il en résulte de plus la remarquable circonstance que, lorsqu'on détermine le nombre  $A$  de cette manière,  $A + 1$  est toujours un multiple de 3.

Pour les premiers nombres premiers du genre considéré on obtient p. e.

$p = 7$	$n = 2$	$A = - 1$	$28 = 1^2 + 27.1^2$
$p = 13$	$n = 4$	$A = + 5$	$52 = 5^2 + 27.1^2$
$p = 19$	$n = 6$	$A = - 7$	$76 = 7^2 + 27.1^2$
$p = 31$	$n = 10$	$A = - 4$	$124 = 4^2 + 27.2^2$
$p = 37$	$n = 12$	$A = + 11$	$148 = 11^2 + 27.1^2$
$p = 43$	$n = 14$	$A = + 8$	$172 = 8^2 + 27.2^2$
$p = 61$	$p = 20$	$A = - 1$	$244 = 1^2 + 27.3^2$

La preuve de ce théorème, qui est étroitement lié aux propriétés de l'équation algébrique d'où dépend la division de la circonférence du cercle en  $p$  parties, se trouve chez Cauchy dans son Mémoire sur la théorie des nombres (Mém. de l'Acad. d. Sc., t. 17, 1840) et chez Lebesgue dans le Journal de Liouville, t. 2, p. 279. Pour plus de détails je renvoie à Bachmann: Die Lehre von der Kreistheilung, p. 144.

Une autre démonstration de ce théorème de Jacobi a été donnée dans l'article „Contribution à la théorie des résidus cubiques et bi-quadratiques” dans le 17<sup>ième</sup> tome des Verslagen en Mededeelingen der Koninklijke Akademie van Wetenschappen, p. 416, n<sup>o</sup> 40.

Je désire ici, en prenant pour point de départ les développements contenus dans cet article, tirer du théorème de Jacobi une détermination directe de la racine  $c$  du carré simple qui figure dans l'équation (1). Il paraîtra que  $c$  est le résidu situé entre  $-\frac{1}{2}p$  et  $+\frac{1}{2}p$  que l'on obtient en divisant par  $p$  le nombre entier

$$2^{n-1} \frac{(n+1)(n+2) \dots (2n)}{1.2.3 \dots n},$$

tandis que  $c-1$  est un multiple de 3.

Par exemple

$p = 7$	$n = 2$	$c = - 2$	$7 = 2^2 + 3.1^2$
$p = 13$	$n = 4$	$c = + 1$	$13 = 1^2 + 3.2^2$
$p = 19$	$n = 6$	$c = + 4$	$19 = 4^2 + 3.1^2$
$p = 31$	$n = 10$	$c = - 2$	$31 = 2^2 + 3.3^2$
$p = 37$	$n = 12$	$c = - 5$	$37 = 5^2 + 3.2^2$

Supposons donc, comme dans l'article cité, que  $\varrho$  soit une racine cubique primitive de l'unité,  $a + b\varrho$  un facteur primaire de  $p$ , et conséquemment

$$p = (a + b\varrho)(a + b\varrho^2) = a^2 - ab + b^2,$$

$a + 1$  et  $b$  sont l'un et l'autre un multiple de 3. Supposons de plus que  $f$  soit l'une des deux racines de la congruence

$$1 + x + x^2 \equiv 0 \pmod{p}$$

le nombre  $f$  étant choisi de telle manière que  $a + bf$  soit divisible par  $p$ .

D'après le théorème de Jacobi cité plus haut, on a alors

$$\dots \quad 2a - b \equiv -\frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p}$$

et plus, en vertu des critères du caractère cubique du nombre 2, on a

$$2^n \equiv 1$$

si  $b$  est pair

$$2^n \equiv f \pmod{p}$$

si  $a$  est pair,

$$2^n \equiv f^2$$

si  $a$  et  $b$  sont impairs tous les deux. (Consultez la p. 398 du mémoire cité.)

Ces trois cas doivent être considérés séparément.

I.  $b$  est pair.

Dans ce cas l'équation

$$p = a^2 - ab + b^2$$

se conduit à

$$\begin{aligned} 4p &= (2a - b)^2 + 3b^2 \\ &= (a - \tfrac{1}{2}b)^2 + 3(\tfrac{1}{2}b)^2. \end{aligned}$$

Dans l'équation (1) on peut donc prendre

$$c = -(a - \tfrac{1}{2}b),$$

et de l'équation (3) l'on tire alors

$$c \equiv \tfrac{1}{2} \cdot \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p}$$

ou bien, comme dans ce cas  $2^n \equiv 1$ ,

$$4^a) \quad . \quad . \quad . \quad c \equiv 2^{n-1} \frac{(n+1)(n+2) \dots (2n)}{1.2.3 \dots n} \pmod{p}.$$

Des équations  $a \equiv 2, b \equiv 0 \pmod{5}$  on tire ensuite

$$5^a) \quad . \quad . \quad . \quad . \quad . \quad c \equiv 1 \pmod{3}.$$

II.  $a$  est pair.

Et ce cas nous remplaçons l'équation

$$p = a^2 - ab + b^2$$

par l'équation

$$16p = (2a - 4b)^2 + 3(2a)^2$$

ou

$$p = \left(\frac{1}{2}a - b\right)^2 + 3\left(\frac{1}{2}a\right)^2,$$

de sorte que dans l'équation (1) nous pouvons prendre

$$c = \frac{1}{2}a - b.$$

Or, on a

$$3) \quad (a + bf)(1 + 2f) \equiv a - 2b + (2a - b)f \equiv -a - b - (2a - b)f^2 \pmod{p}$$

et  $a + bf \equiv 0 \pmod{p}$ . Par conséquent

$$a - 2b \equiv -f(2a - b).$$

On tire donc de l'équation (3)

$$a - 2b \equiv f \frac{(n+1)(n+2) \dots (2n)}{1.2.3 \dots n},$$

ou bien, vu qu'ici  $f \equiv 2^n$ ,

$$b) \quad . \quad . \quad . \quad c \equiv 2^{n-1} \frac{(n+1)(n+2) \dots (2n)}{1.2.3 \dots n} \pmod{p}.$$

Des équations  $a \equiv 2$  et  $b \equiv 0 \pmod{3}$  on conclut en outre

$$b) \quad . \quad . \quad . \quad . \quad . \quad c \equiv 1 \pmod{3}.$$

III.  $a$  et  $b$  sont impairs.

Dans ce dernier cas on a

$$16p = (2a + 2b)^2 + 3(2a - 2b)^2,$$

ou bien

$$p = \left(\frac{a+b}{2}\right)^2 + 3\left(\frac{a-b}{2}\right)^2,$$

te qu'on peut prendre

$$c = \frac{a+b}{2}.$$

tire maintenant de l'équation (6)  $a+b \equiv -f^2(2a-b)$ ; l'équation (3) donne donc

$$a+b \equiv f^2 \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p}.$$

comme en ce cas  $2^n \equiv f^2$ , il s'ensuit que

$$\dots c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p},$$

qu'on voit aisément

$$\dots c \equiv 1 \pmod{3}.$$

équations (4<sup>a</sup>), (4<sup>b</sup>), (4<sup>c</sup>), (5<sup>a</sup>), (5<sup>b</sup>) et (5<sup>c</sup>) et (5<sup>c</sup>) font voir qu'on a dans ces cas

$$\dots c \equiv 2^{n-1} \frac{(n+1)(n+2)\dots(2n)}{1.2.3\dots n} \pmod{p}$$

$$\dots c \equiv 1 \pmod{3},$$

fournit le théorème énoncé plus haut.

peut donner encore une autre forme à la congruence (4). Comme pair, on peut remplacer ce nombre par  $2m$ ; alors

$$c \equiv 2^{2m-1} \frac{(2m+1)(2m+2)\dots(4m)}{1.2.3\dots(2m)}.$$

on a

$$\begin{aligned} 2m+1 &\equiv -(4m), & 2m+3 &\equiv -(4m-2), \\ 2m+5 &\equiv -(4m-4) \dots \text{etc.} \end{aligned}$$

aide de ces équations on obtient

$$c \equiv (-1)^m 2^{2m-1} \frac{[(2m+2)(2m+4)\dots(4m)]^2}{1.2.3\dots(2m)},$$

n, après une réduction facile,

$$c \equiv (-1)^m 2^{4m-1} \frac{(m+1)(m+2)\dots(2m)}{1.2.3\dots m}.$$

On a de plus

$$2^{3m} = 2^{\frac{p-1}{2}} \equiv (-1)^{\frac{p^2-1}{8}}$$

et

$$\frac{p^2-1}{8} = \frac{9m^2+3m}{2}.$$

Retranchant de cet exposant le nombre pair  $\frac{8m^2+4m}{2}$ , on peut écrire plus simplement

$$2^{3m} \equiv (-1)^{\frac{m^2-m}{2}},$$

donc enfin

$$7) \quad c \equiv (-1)^{\frac{m^2+m}{2}} 2^{m-1} \frac{(m+1)(m+2)\dots(2m)}{1 \cdot 2 \cdot 3 \dots m} \pmod{p=6m+1}$$

Cette dernière congruence qui détermine le nombre  $c$  a été donnée sans preuve par Oltramare dans le 87<sup>ième</sup> tome des Comptes rendus de l'Acad. d. Sc., p. 735, en même temps que d'autres formules analogues. Mais cet auteur n'a pas déterminé le signe de  $c$ .

---



## XXVI.

arlem, Arch Néerl. Sci. Soc Holl., 19, 1884, 372—390.)

ote sur le déplacement d'un système invariable dont  
un point est fixe.

On sait depuis Euler que ce déplacement se ramène toujours  
rotation autour d'un axe qui reste fixe.

ieurs auteurs ont établi ce théorème d'une manière purement  
rique; je citerai en particulier Duhamel, qui a traité de ce  
dans l'introduction de son Cours de mécanique.

e reviens sur cette matière, c'est pour mettre en lumière une  
té inhérente à l'analyse suivie par Duhamel. On verra en effet  
s formules données par cet auteur pour déterminer la position  
xe de rotation, cessent de donner cette position dans un cas  
e est cependant parfaitement déterminée — je parle du cas où  
lacement se ramène à une rotation de  $180^\circ$ .

O le point fixe,  $Ox, Oy, Oz$  les axes d'un système de coordon-  
rectangulaires fixe dans l'espace,  $Ox_1, Oy_1, Oz_1$  ceux d'un système  
ordonnées rectangulaires lié au système invariable. Les cosinus  
gles que forment entre eux les axes de ces deux systèmes de  
nnées rectangulaires se trouvent réunis dans le tableau

	$x_1$	$y_1$	$z_1$	
$x$	$a$	$b$	$c$	(A)
$y$	$a'$	$b'$	$c'$	
$z$	$a''$	$b''$	$c''$	

Ces valeurs se rapportent à la première position du système invariable. Pour la seconde position nous écrivons  $a + \Delta a$ ,  $b + \Delta b$ , ...,  $c'' + \Delta c''$  au lieu de  $a$ ,  $b$ , ...,  $c''$ .

Nous supposons qu'on peut faire coïncider les directions positives des  $x_1$ ,  $y_1$ ,  $z_1$  avec celles des  $x$ ,  $y$ ,  $z$ ; on sait qu'alors le déterminant formé avec les neuf quantités  $a$ ,  $b$ , ...,  $c''$  du tableau (A) est égal à  $\pm 1$ .

Je rappelle quelques relations entre ces diverses quantités :

$$\begin{aligned} a &= b' c'' - b'' c', \\ 1 &= a^2 + a'^2 + a''^2, \\ 0 &= ab + a' b' + a'' b''. \end{aligned}$$

Pour abrégé, je ferai usage d'un signe sommatoire  $\Sigma$  qui aura rapport à trois termes, que l'on déduit de celui qui est écrit en laissant l'accent simple et double; p. e., les deux dernières relations sont  $1 = \Sigma a^2$ ,  $0 = \Sigma ab$ . Un chiffre placé à la suite d'une formule indiquera le nombre total de formules analogues qu'on peut en déduire par un changement, soit des lettres  $a$ ,  $b$ ,  $c$ , soit des accents.

Il est clair qu'on a entre les quantités  $a + \Delta a$ , ...,  $c'' + \Delta c''$  les mêmes relations qu'entre  $a$ ,  $b$ , ...,  $c''$ . En combinant ces diverses relations on peut en déduire un grand nombre d'autres; je réunis ici quelques relations simples dont nous aurons surtout besoin

$$1) \quad . \quad . \quad . \quad . \quad . \quad a = b' c'' - b'' c', \quad [9]$$

$$2) \quad . \quad . \quad . \quad . \quad . \quad 2 \Sigma a \Delta a + \Sigma \Delta a^2 = 0, \quad [3]$$

$$3) \quad . \quad . \quad . \quad . \quad . \quad \Sigma a \Delta b + \Sigma b \Delta a + \Sigma \Delta a \Delta b = 0. \quad [3]$$

### *Existence et détermination de l'axe de rotation.*

2. Cela posé, les relations

$$1) \quad . \quad . \quad . \quad . \quad . \quad . \quad \begin{cases} x = a x_1 + b y_1 + c z_1, \\ y = a' x_1 + b' y_1 + c' z_1, \\ z = a'' x_1 + b'' y_1 + c'' z_1, \end{cases}$$

combinées avec les équations analogues pour la seconde position du système, donnent

$$\dots \left\{ \begin{array}{l} \Delta x = x_1 \Delta a + y_1 \Delta b + z_1 \Delta c, \\ \Delta y = x_1 \Delta a' + y_1 \Delta b' + z_1 \Delta c', \\ \Delta z = x_1 \Delta a'' + y_1 \Delta b'' + z_1 \Delta c'', \end{array} \right.$$

gnant par  $x + \Delta x$ ,  $y + \Delta y$ ,  $z + \Delta z$  les coordonnées du point  
ré après le déplacement. Voyons maintenant s'il y a des points  
nt pas changé de position; on devra avoir

$$\dots \left\{ \begin{array}{l} 0 = x_1 \Delta a + y_1 \Delta b + z_1 \Delta c, \\ 0 = x_1 \Delta a' + y_1 \Delta b' + z_1 \Delta c', \\ 0 = x_1 \Delta a'' + y_1 \Delta b'' + z_1 \Delta c''. \end{array} \right.$$

u'il soit possible de satisfaire à ces relations par des valeurs  
 $y_1$ ,  $z_1$  qui ne sont pas toutes égales à zéro, il faut et il suffit  
déterminant

$$\dots D = \begin{vmatrix} \Delta a & \Delta b & \Delta c \\ \Delta a' & \Delta b' & \Delta c' \\ \Delta a'' & \Delta b'' & \Delta c'' \end{vmatrix}.$$

al à zéro. Si cette condition est remplie, les trois plans re-  
és par les équations (6) passent par une même ligne, l'axe  
tion, dont la position est parfaitement déterminée, du moins  
que les neuf mineurs du second degré de D ne sont pas tous  
à zéro.

osition I.

éterminant D est toujours égal à zéro.

osition II.

neuf mineurs du second degré de D sont tous égaux à zéro,  
ent dans le cas qu'on a  $\Delta a = 0$ ,  $\Delta b = 0$ , ...,  $\Delta c'' = 0$ ,  
lire quand il n'y a pas de déplacement.

ynons par  $D_a$ ,  $D_b$ , ...,  $D_c$  les mineurs de D, en sorte qu'on a

$$\dots \left\{ \begin{array}{l} D = \Sigma \Delta a D_a = \Sigma \Delta b D_b = \Sigma \Delta c D_c \\ 0 = \Sigma \Delta a D_b = \Sigma \Delta b D_c = \Sigma \Delta c D_a. \end{array} \right.$$

eur de  $D_a$  est  $\Delta b' \Delta c'' - \Delta b'' \Delta c'$ , mais l'équation (1) donne  
 $= b' \Delta c'' - b'' \Delta c' + c'' \Delta b' - c' \Delta b'' + \Delta b' \Delta c'' - \Delta b'' \Delta c'$ ,

$$a = \Delta a - b' \Delta c'' + b'' \Delta c' - c'' \Delta b' + c' \Delta b'', \quad [3]$$

$$a' = \Delta a' - b'' \Delta c + b \Delta c'' - c \Delta b'' + c'' \Delta b, \quad [3]$$

$$a'' = \Delta a'' - b \Delta c' + b' \Delta c - c' \Delta b + c \Delta b'. \quad [3]$$

On en déduit, en multipliant par  $\Delta a$ ,  $\Delta a'$ ,  $\Delta a''$  et faisant l'addition

$$0) \quad \dots \quad D = \Sigma \Delta a^2 - \Sigma b D_b - \Sigma c D_c. \quad [3]$$

Mais en multipliant les équations (9) par  $a$ ,  $a'$ ,  $a''$  on trouvera par addition, en vertu des relations (1)

$$\Sigma a D_a = \Sigma a \Delta a - \Sigma b \Delta b - \Sigma c \Delta c,$$

ou bien, à cause de (2)

$$1) \quad \dots \quad \begin{cases} \Sigma a D_a = -\frac{1}{2} \Sigma \Delta a^2 + \frac{1}{2} \Sigma \Delta b^2 + \frac{1}{2} \Sigma \Delta c^2, \\ \Sigma b D_b = +\frac{1}{2} \Sigma \Delta a^2 - \frac{1}{2} \Sigma \Delta b^2 + \frac{1}{2} \Sigma \Delta c^2, \\ \Sigma c D_c = +\frac{1}{2} \Sigma \Delta a^2 + \frac{1}{2} \Sigma \Delta b^2 - \frac{1}{2} \Sigma \Delta c^2. \end{cases}$$

En substituant ces valeurs de  $\Sigma b D_b$ ,  $\Sigma c D_c$  dans l'équation (10) on obtient

$$D = 0, \quad c. q. f. d.$$

Les équations (11), qui donnent

$$2) \quad \Sigma a D_a + \Sigma b D_b + \Sigma c D_c = \frac{1}{2} \Sigma \Delta a^2 + \frac{1}{2} \Sigma \Delta b^2 + \frac{1}{2} \Sigma \Delta c^2,$$

on voit bien qu'en supposant  $D_a = D_b = \dots = D_c = 0$  on doit avoir :  $\Sigma \Delta a^2 = 0$ ,  $\Sigma \Delta b^2 = 0$ ,  $\Sigma \Delta c^2 = 0$ , donc  $\Delta a = \Delta b = \dots = \Delta c'' = 0$ , ce qui est notre proposition II.

D'après la démonstration qui précède, il est bien évident que la proposition I est une conséquence nécessaire des relations auxquelles ces quantités

$$\begin{array}{ll} a, & b, & c & a + \Delta a, & b + \Delta b, & c + \Delta c \\ a', & b', & c' & a' + \Delta a', & b' + \Delta b', & c' + \Delta c' \\ a'', & b'', & c'' & a'' + \Delta a'', & b'' + \Delta b'', & c'' + \Delta c'' \end{array}$$

sont soumises, en sorte que cette proposition reste vraie quelles que soient ces quantités, réelles ou non. La proposition II, au contraire, est démontrée seulement en supposant réelles les quantités  $\Delta a$ ,  $\Delta b$ ,  $\dots$ ,  $\Delta c''$ . Nous reviendrons plus tard sur cette proposition II, pour faire voir qu'elle aussi est une conséquence des relations entre les  $\dots$ ,  $c''$ ,  $\Delta a$ ,  $\dots$ ,  $\Delta c''$  et ne dépend nullement de la réalité de ces dernières quantités.

Après ce qui précède, l'axe de rotation est parfaitement déterminé par

$$\left. \begin{aligned} x_1 : y_1 : z_1 &= D_a : D_b : D_c \\ &= D_{a'} : D_{b'} : D_{c'} \\ &= D_{a''} : D_{b''} : D_{c''} \end{aligned} \right\}$$

cette détermination devient illusoire seulement quand il n'y a pas de mouvement. Ajoutons encore les relations suivantes, qui nous seront utiles plus tard et que l'on obtient sans difficulté en partant des équations (9) et faisant attention aux relations (3)

$$\dots \quad \Sigma b D_a = \Sigma a D_b = -\Sigma \Delta a \Delta b. \quad [3]$$

On obtient encore une expression remarquable pour la somme  $+\Sigma D_b^2 + \Sigma D_c^2$ . En effet, on a d'après (11) et (14)

$$\begin{aligned} \Sigma a D_a &= -A + B + C, \\ \Sigma b D_a &= -\Sigma \Delta a \Delta b, \\ \Sigma c D_a &= -\Sigma \Delta a \Delta c, \end{aligned}$$

On a posé, pour abrégé,  $\frac{1}{2} \Sigma \Delta a^2 = A$ ,  $\frac{1}{2} \Sigma \Delta b^2 = B$ ,  $\frac{1}{2} \Sigma \Delta c^2 = C$ . La somme des carrés de ces trois équations donne

$$\Sigma D_a^2 = (-A + B + C)^2 + (\Sigma \Delta a \Delta b)^2 + (\Sigma \Delta a \Delta c)^2.$$

On a, d'après une transformation bien connue

$$\begin{aligned} 4AB &= \Sigma \Delta a^2 \times \Sigma \Delta b^2 = (\Sigma \Delta a \Delta b)^2 + D_c^2 + D_c'^2 + D_c''^2 \\ 4AC &= \Sigma \Delta a^2 \times \Sigma \Delta c^2 = (\Sigma \Delta a \Delta c)^2 + D_b^2 + D_b'^2 + D_b''^2, \end{aligned}$$

$$\Sigma D_a^2 + \Sigma D_b^2 + \Sigma D_c^2 = (A + B + C)^2,$$

Autrement dit

$$\Sigma D_a^2 + \Sigma D_b^2 + \Sigma D_c^2 = \frac{1}{4} [\Sigma \Delta a^2 + \Sigma \Delta b^2 + \Sigma \Delta c^2]^2.$$

*Autre formule pour déterminer l'axe de rotation.*

D'après ce qui précède, on a

$$\begin{aligned} D &= \Delta a D_a + \Delta b D_b + \Delta c D_c = 0, \\ \Delta a' D_a + \Delta b' D_b + \Delta c' D_c &= 0, \\ \Delta a'' D_a + \Delta b'' D_b + \Delta c'' D_c &= 0. \end{aligned}$$

En multipliant ces équations par  $c + \frac{1}{2} \Delta c$ ,  $c' + \frac{1}{2} \Delta c'$ ,  $c'' + \frac{1}{2} \Delta c''$  la quantité  $D_c$  se trouvera éliminée après l'addition, en vertu des relations (2). En posant donc

$$6) \quad \left\{ \begin{array}{l} p = \Sigma (c + \frac{1}{2} \Delta c) \Delta b = - \Sigma (b + \frac{1}{2} \Delta b) \Delta c \\ q = \Sigma (a + \frac{1}{2} \Delta a) \Delta c = - \Sigma (c + \frac{1}{2} \Delta c) \Delta a \\ r = \Sigma (b + \frac{1}{2} \Delta b) \Delta a = - \Sigma (a + \frac{1}{2} \Delta a) \Delta b \end{array} \right.$$

obtient  $-q D_a + p D_b = 0$  ou  $D_a : D_b = p : q$ . En réunissant toutes les relations de même nature, on trouve

$$7) \quad \left\{ \begin{array}{l} p : q : r = D_a : D_b : D_c \\ \quad \quad \quad = D_{a'} : D_{b'} : D_{c'} \\ \quad \quad \quad = D_{a''} : D_{b''} : D_{c''} \end{array} \right.$$

Par conséquent la formule (13), qui détermine l'axe de rotation, peut se mettre sous la forme

$$8) \quad x_1 : y_1 : z_1 = p : q : r.$$

C'est la formule donnée par Duhamel. Elle devient illusoire quand on a à la fois  $p=0$ ,  $q=0$  et  $r=0$ . Nous verrons que cela a lieu non seulement quand il n'y a pas de déplacement, mais encore dans d'autres cas. Alors cette formule (18) devient insuffisante et il faut recourir aux formules (13). Nous allons déduire maintenant un système de formules qui nous permettra de dire avec précision dans quels cas on a :  $p=0$ ,  $q=0$ ,  $r=0$ .

4. Nous avons

$$\begin{aligned} 0 &= (a + \frac{1}{2} \Delta a) \Delta a + (a' + \frac{1}{2} \Delta a') \Delta a' + (a'' + \frac{1}{2} \Delta a'') \Delta a'' \\ + r &= (b + \frac{1}{2} \Delta b) \Delta a + (b' + \frac{1}{2} \Delta b') \Delta a' + (b'' + \frac{1}{2} \Delta b'') \Delta a'' \\ - q &= (c + \frac{1}{2} \Delta c) \Delta a + (c' + \frac{1}{2} \Delta c') \Delta a' + (c'' + \frac{1}{2} \Delta c'') \Delta a''. \end{aligned}$$

En éliminant  $\Delta a'$ ,  $\Delta a''$  il vient

$$9) \quad R \Delta a = r R_b - q R_c \quad [9]$$

désignant par  $R$  le déterminant

$$10) \quad R = \begin{vmatrix} a + \frac{1}{2} \Delta a & b + \frac{1}{2} \Delta b & c + \frac{1}{2} \Delta c \\ a' + \frac{1}{2} \Delta a' & b' + \frac{1}{2} \Delta b' & c' + \frac{1}{2} \Delta c' \\ a'' + \frac{1}{2} \Delta a'' & b'' + \frac{1}{2} \Delta b'' & c'' + \frac{1}{2} \Delta c'' \end{vmatrix}$$

par  $R_a, R_b, \dots, R_c$  les mineurs du second degré de  $R$ .

la valeur de  $R_a$  est  $(b' + \frac{1}{2} \Delta b')(c'' + \frac{1}{2} \Delta c'') - (b'' + \frac{1}{2} \Delta b'')(c' + \frac{1}{2} \Delta c')$   
opérant les multiplications on peut simplifier le résultat à l'aide  
la relation (1) et de la valeur de  $\Delta a$  qu'on en tire; on trouvera

$$R_a = a + \frac{1}{2} \Delta a - \frac{1}{4} (\Delta b' \Delta c'' - \Delta b'' \Delta c'),$$

d.

$$\dots \dots \dots R_a = a + \frac{1}{2} \Delta a - \frac{1}{4} D_a. \quad [9]$$

on en tire aussitôt

$$\dots \dots \dots \Sigma R_a \Delta a = 0, \quad [3]$$

$$\dots \dots \dots \Sigma R_a \Delta b = -r, \quad [3]$$

$$\dots \dots \dots \Sigma R_a \Delta c = +q. \quad [3]$$

l'équation (19) donne ensuite

$$R \Sigma \Delta a^2 = r \Sigma R_b \Delta a - q \Sigma R_c \Delta a,$$

$$R \Sigma \Delta a \Delta b = r \Sigma R_b \Delta b - q \Sigma R_c \Delta b,$$

c'est-à-dire, en vertu des relations (22), (23), (24)

$$\dots \dots \dots \begin{cases} R \Sigma \Delta a^2 = q^2 + r^2, & R \Sigma \Delta a \Delta b = -pq, \\ R \Sigma \Delta b^2 = r^2 + p^2, & R \Sigma \Delta b \Delta c = -qr, \\ R \Sigma \Delta c^2 = p^2 + q^2, & R \Sigma \Delta c \Delta a = -rp, \end{cases}$$

on voit, en faisant attention aux formules (11) et (14)

$$\dots \dots \dots \begin{cases} p^2 = R \Sigma a D_a, \\ q^2 = R \Sigma b D_b, \\ r^2 = R \Sigma c D_c. \end{cases}$$

$$\dots \dots \dots \begin{cases} qr = R \Sigma b D_c = R \Sigma c D_b, \\ rp = R \Sigma c D_a = R \Sigma a D_c, \\ pq = R \Sigma a D_b = R \Sigma b D_a. \end{cases}$$

Nous pouvons maintenant exprimer aussi les  $D_a, \dots, D_c$  à l'aide  
 $p, q, r$ ; — en effet, les formules

$$R(a D_a + a' D_{a'} + a'' D_{a''}) = p^2,$$

$$R(b D_a + b' D_{a'} + b'' D_{a''}) = pq,$$

$$R(c D_a + c' D_{a'} + c'' D_{a''}) = pr$$

donnent aussitôt la première des neuf équations

$$\left\{ \begin{array}{l} R D_a = p(a p + b q + c r), \quad R D_b = q(a p + b q + c r), \\ R D_{a'} = p(a' p + b' q + c' r), \quad R D_{b'} = q(a' p + b' q + c' r), \\ R D_{a''} = p(a'' p + b'' q + c'' r), \quad R D_{b''} = q(a'' p + b'' q + c'' r), \\ R D_c = r(a p + b q + c r), \\ R D_{c'} = r(a' p + b' q + c' r), \\ R D_{c''} = r(a'' p + b'' q + c'' r). \end{array} \right.$$

après la définition des  $R_a, \dots, R_{c''}$ , on a  $R = \Sigma(a + \frac{1}{2} \Delta a) R_a$ , ou en, à cause de (22),  $R = \Sigma a R_a$ . En substituant la valeur (21) de il vient

$$R = 1 + \frac{1}{2} \Sigma a \Delta a - \frac{1}{4} \Sigma a D_a = 1 - \frac{1}{4} \Sigma \Delta a^2 - \frac{1}{4} \Sigma a D_a,$$

bien, parce que les relations (11) donnent  $\Sigma \Delta a^2 = \Sigma b D_b + \Sigma c D_c$ ,

$$R = 1 - \frac{1}{4} \Sigma a D_a - \frac{1}{4} \Sigma b D_b - \frac{1}{4} \Sigma c D_c.$$

On tire des équations (26)

$$p^2 + q^2 + r^2 = R(\Sigma a D_a + \Sigma b D_b + \Sigma c D_c);$$

le facteur de  $R$  dans le second membre est égal à  $4(1 - R)$  d'après (27), donc

$$p^2 + q^2 + r^2 = 4 R(1 - R).$$

La relation (21) donne encore  $\Sigma b R_a = \frac{1}{2} \Sigma b \Delta a - \frac{1}{4} \Sigma b D_a$ , ou bien, à cause de (14):  $\Sigma b R_a = \frac{1}{2} \Sigma b \Delta a + \frac{1}{4} \Sigma \Delta a \Delta b$ , c'est-à-dire:  $\Sigma b R_a = \frac{1}{2} r$ .

On obtient de la même manière

$$\left\{ \begin{array}{l} p = 2 \Sigma c R_b = -2 \Sigma b R_c, \\ q = 2 \Sigma a R_c = -2 \Sigma c R_a, \\ r = 2 \Sigma b R_a = -2 \Sigma a R_b. \end{array} \right.$$

Les équations

$$\left\{ \begin{array}{l} a R_a + a' R_{a'} + a'' R_{a''} = R, \\ b R_a + b' R_{a'} + b'' R_{a''} = \frac{1}{2} r, \\ c R_a + c' R_{a'} + c'' R_{a''} = -\frac{1}{2} q \end{array} \right.$$

donnent maintenant la première des neuf relations

$$\left\{ \begin{array}{l} R_a = a R + \frac{1}{2} (b r - c q), \quad R_b = b R + \frac{1}{2} (c p - a r), \\ R_{a'} = a' R + \frac{1}{2} (b' r - c' q), \quad R_{b'} = b' R + \frac{1}{2} (c' p - a' r), \\ R_{a''} = a'' R + \frac{1}{2} (b'' r - c'' q), \quad R_{b''} = b'' R + \frac{1}{2} (c'' p - a'' r), \\ R_c = c R + \frac{1}{2} (a q - b p), \\ R_{c'} = c' R + \frac{1}{2} (a' q - b' p), \\ R_{c''} = c'' R + \frac{1}{2} (a'' q - b'' p). \end{array} \right.$$



omme des carrés des mêmes équations donne

$$\Sigma R_a^2 = R^2 + \frac{1}{4} q^2 + \frac{1}{4} r^2, \quad [3]$$

$$\Sigma R_a^2 + \Sigma R_b^2 + \Sigma R_c^2 = 3 R^2 + \frac{1}{2} (p^2 + q^2 + r^2),$$

à dire, en vertu de (30)

$$\dots \Sigma R_a^2 + \Sigma R_b^2 + \Sigma R_c^2 = R^2 + 2 R.$$

Revenons maintenant à la proposition II, qui a été démontrée  
ement en supposant  $\Delta a, \Delta b, \dots, \Delta c''$  réels Faisons donc :  
 $D_b = \dots = D_c = 0$  et voyons ce qui s'en suit Les équations (29)  
(6) donnent:  $R=1, p=0, q=0, r=0$ . Ensuite les équations (19)

$$\Delta a = 0, \Delta b = 0, \dots, \Delta c'' = 0.$$

omme nous l'avons déjà annoncé cette proposition II ne dépend  
c en aucune façon de la réalité des quantités  $\Delta a, \dots, \Delta c''$ .

Voyons maintenant dans quels cas la formule (18) cesse de  
terminer l'axe de rotation, c'est-à-dire dans quels cas on a  $p=0,$   
 $q=0, r=0$ . La formule (30) fait voir que  $R$  est égal à l'unité ou  
à zéro.

Premier cas:  $R=1, p=0, q=0, r=0$ .

Les relations (28) font voir que tous les  $D_a, \dots, D_c$  deviennent égaux  
à zéro, d'après la proposition II, il s'ensuit que tous les  $\Delta a, \dots, \Delta c''$   
sont aussi égaux à zéro: il n'y a pas de déplacement. L'indétermi-  
nation de l'axe de rotation dans ce cas est aussi annoncée par  
l'équation (13), elle est dans la nature des choses. Les quatre équations  
 $R=1, p=0, q=0, r=0$  vérifiant la relation (30) équivalent  
à trois conditions, qui suffisent à déterminer le déplacement, qui  
est nul, comme on l'a vu. En effet, la condition  $R=1$  donne bien  
 $p^2 + q^2 + r^2 = 0$ , mais algébriquement cela n'entraîne nullement  
 $p=0, q=0, r=0$ , bien que cela ait lieu en admettant seulement  
des valeurs réelles. P. e., supposons que le tableau (A) soit

$$\begin{vmatrix} 1 & 0 & 0 \\ 0 & 1 & 0 \\ 0 & 0 & 1 \end{vmatrix} \quad \text{et après le déplacement} \quad \begin{vmatrix} \frac{3}{2} & \frac{1}{2} i & i \\ \frac{1}{2} i & \frac{1}{2} & -1 \\ -i & 1 & 1 \end{vmatrix} \quad \text{donc}$$

$$\begin{aligned}\Delta a &= \frac{1}{2}, & \Delta b &= \frac{1}{2}i, & \Delta c &= i, \\ \Delta a' &= \frac{1}{2}i, & \Delta b' &= -\frac{1}{2}, & \Delta c' &= -1, \\ \Delta a'' &= -i, & \Delta b'' &= 1, & \Delta c'' &= 0.\end{aligned}$$

on trouvera  $R=1$ ,  $p=1$ ,  $q=i$ ,  $r=0$ .

Il en est tout autrement dans le

Second cas:  $R=0$ ,  $p=0$ ,  $q=0$ ,  $r=0$ .

En effet, les équations (26) montrent que la condition  $R=0$  entraîne déjà ces trois autres:  $p=0$ ,  $q=0$ ,  $r=0$ . Ce second cas est donc caractérisé par la condition unique  $R=0$ , qui ne peut pas déterminer le déplacement, qu'on peut au contraire assujettir encore deux autres conditions.

Pour reconnaître la signification de cette condition  $R=0$ , il faut se reporter aux équations (4) et (5), qui donnent

$$\begin{aligned}x + \frac{1}{2} \Delta x &= (a + \frac{1}{2} \Delta a) x_1 + (b + \frac{1}{2} \Delta b) y_1 + (c + \frac{1}{2} \Delta c) z_1, \\ y + \frac{1}{2} \Delta y &= (a' + \frac{1}{2} \Delta a') y_1 + (b' + \frac{1}{2} \Delta b') y_1 + (c' + \frac{1}{2} \Delta c') z_1, \\ z + \frac{1}{2} \Delta z &= (a'' + \frac{1}{2} \Delta a'') z_1 + (b'' + \frac{1}{2} \Delta b'') y_1 + (c'' + \frac{1}{2} \Delta c'') z_1.\end{aligned}$$

On voit par là que  $R=0$  est la condition nécessaire et suffisante pour qu'il soit possible de satisfaire aux conditions

$$\begin{aligned}x + \frac{1}{2} \Delta x &= 0, \\ y + \frac{1}{2} \Delta y &= 0, \\ z + \frac{1}{2} \Delta z &= 0,\end{aligned}$$

par des valeurs de  $x_1$ ,  $y_1$ ,  $z_1$  qui ne sont pas toutes nulles. Pour tous les points d'une certaine droite passant par l'origine on a alors  $x + \Delta x = -x$ ,  $y + \Delta y = -y$ ,  $z + \Delta z = -z$ , c'est-à-dire, après le déplacement cette droite se retrouve dans sa première position, avec superposition des deux moitiés différentes. Or une considération géométrique bien simple montre que le déplacement consiste alors dans une rotation de  $180^\circ$  autour d'un certain axe, et que toutes les droites passant par l'origine et situées dans un plan perpendiculaire à l'axe de rotation jouissent de la propriété énoncée. Ainsi, lorsque  $R=0$ , les trois plans

$$\begin{aligned}(a + \frac{1}{2} \Delta a) x_1 + (b + \frac{1}{2} \Delta b) y_1 + (c + \frac{1}{2} \Delta c) z_1 &= 0, \\ (a' + \frac{1}{2} \Delta a') x_1 + (b' + \frac{1}{2} \Delta b') y_1 + (c' + \frac{1}{2} \Delta c') z_1 &= 0, \\ (a'' + \frac{1}{2} \Delta a'') x_1 + (b'' + \frac{1}{2} \Delta b'') y_1 + (c'' + \frac{1}{2} \Delta c'') z_1 &= 0\end{aligned}$$

nt non seulement par une même droite, mais ces trois plans  
dent avec un plan mené par l'origine perpendiculairement à  
de rotation Autrement, et dans le langage de l'algèbre nous  
ns énoncer cette :

osition III. Lorsque le déterminant  $R$  est égal à zéro, ces  
mineurs  $R_a, R_b, \dots, R_c$  s'évanouissent en même temps

effet, la supposition  $R=0$  donne  $p=0, q=0, r=0$ , et dès  
es équations (32) mettent en évidence notre proposition. Cette  
nstration, on le voit, ne dépend nullement de la réalité des  
ités  $a, b, \dots, \Delta a, \Delta b, \dots$ , comme la considération géométrique  
ous a conduit d'abord à cette proposition. Dans le cas actuel,  
ation (21) donne encore :  $D_a = 4(a + \frac{1}{2} \Delta a)$  etc., en sorte que  
tion (13) de l'axe de rotation peut s'écrire

$$\left\{ \begin{aligned} x_1 : y_1 : z_1 &= a + \frac{1}{2} \Delta a : b + \frac{1}{2} \Delta b : c + \frac{1}{2} \Delta c, \\ &= a' + \frac{1}{2} \Delta a' : b' + \frac{1}{2} \Delta b' : c' + \frac{1}{2} \Delta c', \\ &= a'' + \frac{1}{2} \Delta a'' : b'' + \frac{1}{2} \Delta b'' : c'' + \frac{1}{2} \Delta c'', \end{aligned} \right.$$

est bien conforme à ce que nous venons de dire.

y a pas lieu de s'occuper du sens de la rotation, parce qu'une  
on de  $180^\circ$  dans l'un ou l'autre sens produit le même effet.

Après avoir traité complètement le cas  $p=0, q=0, r=0$   
en ferons abstraction dans la suite, et par conséquent l'axe  
rotation sera déterminé par l'équation (18). Il nous reste à déter-  
l'amplitude et le sens de la rotation qui permet de passer de  
ième position du système invariable à la seconde position.

et  $\theta$  l'amplitude de la rotation; comme une rotation  $\theta$  dans  
sens produit le même effet qu'une rotation  $360^\circ - \theta$  effectuée  
le sens contraire, nous pouvons supposer la valeur absolue  
inférieure à  $180^\circ$ . Prenons un point arbitraire  $P$  sur l'axe  
rotation et une droite  $OQ$  perpendiculaire à  $OP$  et liée au  
ne invariable. Pour amener la droite  $OQ$  dans sa position finale,  
et la tourner d'un angle  $\theta < 180^\circ$  autour de  $OP$ , dans un certain  
Supposons que par une rotation de  $90^\circ$  dans le même sens,  
ite  $OQ$  vienne dans la position  $OR$ . Alors nous conviendrons  
nsidérer l'angle  $\theta$  comme positif ou négatif selon que les trois

droites  $OP$ ,  $OQ$ ,  $OR$  ont ou n'ont pas la même disposition que les axes  $Ox$ ,  $Oy$ ,  $Oz$ . Nous avons pris arbitrairement la direction  $OP$  pour l'axe de rotation. On voit qu'en prenant la direction opposée, le signe de  $\Theta$  change.

Supposons  $OQ$  égal à l'unité et  $OQ'$  la position finale de  $OQ$ , on voit immédiatement que

$$QQ'^2 = 4 \sin^2 \frac{1}{2} \Theta,$$

et cette équation détermine complètement la valeur absolue de  $\Theta$ .

Soient  $x_1, y_1, z_1$  les coordonnées de  $Q$  par rapport aux axes  $Ox_1, Oy_1, Oz_1$ . Les équations (5) donnent

$$\begin{aligned} QQ'^2 = \Delta x^2 + \Delta y^2 + \Delta z^2 = & x_1^2 \Sigma \Delta a^2 + 2 y_1 z_1 \Sigma \Delta b \Delta c \\ & + y_1^2 \Sigma \Delta b^2 + 2 z_1 x_1 \Sigma \Delta c \Delta a \\ & + z_1^2 \Sigma \Delta c^2 + 2 x_1 y_1 \Sigma \Delta a \Delta b. \end{aligned}$$

En multipliant par  $R$  nous trouvons, en faisant attention aux relations (25)

$$\begin{aligned} R(\Delta x^2 + \Delta y^2 + \Delta z^2) = & (q^2 + r^2) x_1^2 - 2 q r y_1 z_1 \\ & + (r^2 + p^2) y_1^2 - 2 r p z_1 x_1 \\ & + (p^2 + q^2) z_1^2 - 2 p q x_1 y_1 = \\ & (p^2 + q^2 + r^2)(x_1^2 + y_1^2 + z_1^2) - (p x_1 + q y_1 + r z_1)^2. \end{aligned}$$

Mais on a  $p x_1 + q y_1 + r z_1 = 0$ , à cause de la perpendicularité de  $OP$  et  $OQ$ , et  $x_1^2 + y_1^2 + z_1^2 = 1$ ; donc

$$4 R \sin^2 \frac{1}{2} \Theta = p^2 + q^2 + r^2 = 4 R (1 - R).$$

Nous arrivons donc à l'expression suivante, qui détermine la valeur absolue de  $\Theta$

$$(35) \quad \sin^2 \frac{1}{2} \Theta = 1 - R.$$

Il faut encore déterminer le signe de  $\Theta$ . Pour cela, soit  $OP = 1$ , et soient

$$\begin{array}{ccc} X_1, & Y_1, & Z_1 \\ X_2, & Y_2, & Z_2 \\ X_3, & Y_3, & Z_3 \end{array}$$

les coordonnées de  $P, Q, Q'$  par rapport aux axes  $Ox_1, Oy_1, Oz_1$  (dans leur position initiale). Le déterminant

$$\begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix}$$

alors égal en valeur absolue au sextuple de la pyramide O P Q Q',  
c'est-à-dire égal à  $\pm \sin \theta$ , et, d'après la manière dont nous détermi-  
nons le signe de  $\theta$ , le signe de ces deux expressions est encore  
le même, donc

$$\sin \theta = \begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 & Y_3 & Z_3 \end{vmatrix} = \begin{vmatrix} X_1 & Y_1 & Z_1 \\ X_2 & Y_2 & Z_2 \\ X_3 - X_2 & Y_3 - Y_2 & Z_3 - Z_2 \end{vmatrix}$$

$$\sin \theta = (X_3 - X_2)(Y_1 Z_2 - Y_2 Z_1) + (Y_3 - Y_2)(Z_1 X_2 - Z_2 X_1) \\ + (Z_3 - Z_2)(X_1 Y_2 - X_2 Y_1).$$

en posant  $S = \sqrt{p^2 + q^2 + r^2}$ , on aura  $X_1 = \frac{p}{S}$ ,  $Y_1 = \frac{q}{S}$ ,  $Z_1 = \frac{r}{S}$ .

On peut prendre arbitrairement  $S$  positif ou négatif, il faut seu-  
lement conserver dans la suite la valeur adoptée.

Ensuite  $X_3 - X_2$ ,  $Y_3 - Y_2$ ,  $Z_3 - Z_2$  sont évidemment les projections  
sur les axes  $Ox_1$ ,  $Oy_1$ ,  $Oz_1$  de la ligne Q Q'. Or on connaît, par les  
formules (5), les projections de Q Q' sur les axes  $Ox$ ,  $Oy$ ,  $Oz$ ; on en  
conclut

$$\begin{aligned} X_3 - X_2 &= X_2 \Sigma a \Delta a + Y_2 \Sigma a \Delta b + Z_2 \Sigma a \Delta c, \\ Y_3 - Y_2 &= X_2 \Sigma b \Delta a + Y_2 \Sigma b \Delta b + Z_2 \Sigma b \Delta c, \\ Z_3 - Z_2 &= X_2 \Sigma c \Delta a + Y_2 \Sigma c \Delta b + Z_2 \Sigma c \Delta c. \end{aligned}$$

On trouve facilement, à l'aide des équations (2), (16), (25)

$$\begin{aligned} & \dots \dots \dots \begin{cases} R \Sigma a \Delta a = -\frac{1}{2}(q^2 + r^2), \\ R \Sigma b \Delta b = -\frac{1}{2}(r^2 + p^2), \\ R \Sigma c \Delta c = -\frac{1}{2}(p^2 + q^2). \end{cases} \\ & \dots \begin{cases} R \Sigma b \Delta c = -R p + \frac{1}{2} q r, & R \Sigma c \Delta b = +R p + \frac{1}{2} q r, \\ R \Sigma c \Delta a = -R q + \frac{1}{2} r p, & R \Sigma a \Delta c = +R q + \frac{1}{2} r p, \\ R \Sigma a \Delta b = -R r + \frac{1}{2} p q, & R \Sigma b \Delta a = +R r + \frac{1}{2} p q. \end{cases} \end{aligned}$$

introduisant ces valeurs et celles-ci:  $X_1 = \frac{p}{S}$ ,  $Y_1 = \frac{q}{S}$ ,  $Z_1 = \frac{r}{S}$ ,

on aient

$$\begin{aligned}
 R S \sin \Theta = & \left[ -\frac{1}{2} (q^2 + r^2) X_2 + (-R r + \frac{1}{2} p q) Y_2 + (R q + \frac{1}{2} r p) Z_2 \right] \\
 & (q Z_2 - r Y_2) \\
 & + \left[ (R r + \frac{1}{2} p q) X_2 - \frac{1}{2} (r^2 + p^2) Y_2 + (-R p + \frac{1}{2} q r) Z_2 \right] \\
 & (r X_2 - p Z_2) \\
 & + \left[ (-R q + \frac{1}{2} r p) X_2 + (R p + \frac{1}{2} q r) Y_2 - \frac{1}{2} (p^2 + q^2) Z_2 \right] \\
 & (p Y_2 - q X_2).
 \end{aligned}$$

En réduisant, le second membre devient divisible par  $R$  et l'on obtient

$$\begin{aligned}
 S \sin \Theta = & (q^2 + r^2) X_2^2 - 2 q r Y_2 Z_2 \\
 & + (r^2 + p^2) Y_2^2 - 2 r p Z_2 X_2 \\
 & + (p^2 + q^2) Z_2^2 - 2 p q X_2 Y_2
 \end{aligned}$$

et comme tout à l'heure  $S \sin \Theta = p^2 + q^2 + r^2 = S^2$ ; donc définitivement

$$(38) \quad \sin \Theta = S.$$

Les formules (35) et (38), c'est-à-dire

$$\begin{aligned}
 \sin \Theta &= S, \\
 \cos \Theta &= 2 R - 1
 \end{aligned}$$

donnent sans aucune ambiguïté l'angle de rotation  $\Theta$ .

8. La position du système invariable dépend de trois paramètres. Par conséquent, on peut se proposer de déterminer la seconde position en connaissant la première position et les trois quantités  $p, q, r$ . Nous avons à exprimer  $\Delta a, \dots, \Delta c''$  à l'aide de  $p, q, r$  et de  $a, b, c, \dots, c''$ . Les formules que nous avons développées donnent facilement la solution de ce problème. Remarquons d'abord que la quantité  $R$  se détermine à l'aide de la relation  $p^2 + q^2 + r^2 = 4 R (1 - R)$ . On trouve deux valeurs de  $R$  qui se rapportent à deux rotations autour d'un même axe, mais dont les amplitudes sont supplémentaires. Les formules (19) et (32) donnent ensuite

$$(39) \quad R \Delta a = R (b r - c q) + \frac{1}{2} p (a p + b q + c r) - \frac{1}{2} a (p^2 + q^2 + r^2). \quad [9]$$

Voici une autre expression des  $\Delta a, \dots, \Delta c''$  qu'on obtient à l'aide de (21) et (32)

$$(40) \quad \Delta a = b r - c q + \frac{1}{2} D a - 2 a (1 - R). \quad [9]$$

Prenons par  $u, v, w$  les cosinus des angles que la direction  $OP$  fait avec les axes  $Ox_1, Oy_1, Oz_1$ , et par  $k, k', k''$  les cosinus des angles que la même direction fait avec les axes  $Ox, Oy, Oz$ ; on aura, d'après ce qui précède

$$\begin{aligned} p &= u \sin \Theta, & ap + bq + cr &= k \sin \Theta, \\ q &= v \sin \Theta, & a'p + b'q + c'r &= k' \sin \Theta, \\ r &= w \sin \Theta, & a''p + b''q + c''r &= k'' \sin \Theta. \end{aligned}$$

Les équations (28) prennent la forme simple

$$\begin{aligned} (1 - \cos \Theta) uk, \quad D_b &= 2(1 - \cos \Theta) vk, \quad D_c = 2(1 - \cos \Theta) wk, \\ (1 - \cos \Theta) uk', \quad D_{b'} &= 2(1 - \cos \Theta) vk', \quad D_{c'} = 2(1 - \cos \Theta) wk', \\ (1 - \cos \Theta) uk'', \quad D_{b''} &= 2(1 - \cos \Theta) vk'', \quad D_{c''} = 2(1 - \cos \Theta) wk'', \end{aligned}$$

Les formules (40)

$$\Delta a = \sin \Theta (bw - cv) + (1 - \cos \Theta) (uk - a). \quad [9]$$

Les équations (13) et (18) sont celles de l'axe de rotation par rapport aux axes  $Ox_1, Oy_1, Oz_1$ . On obtient des équations aussi simples par rapport aux axes  $Ox, Oy, Oz$ . En effet, on a  $x_1 = ax + a'y + a''z$ ,  $y_1 = ay + a'x + a''z$ ,  $z_1 = az + a'x + a'y$ , et par conséquent l'axe de rotation est déterminé par

$$\begin{aligned} 0 &= x \Delta a + y \Delta a' + z \Delta a'', \\ 0 &= x \Delta b + y \Delta b' + z \Delta b'', \\ 0 &= x \Delta c + y \Delta c' + z \Delta c'', \end{aligned}$$

$$\dots \dots \dots \left\{ \begin{aligned} x : y : z &= D_a : D_{a'} : D_{a''} \\ &= D_b : D_{b'} : D_{b''} \\ &= D_c : D_{c'} : D_{c''}. \end{aligned} \right.$$

Poursuivant cette voie, il faudrait introduire, au lieu de  $p, q, r$ , d'autres quantités  $s, s', s''$  par les équations

$$\left\{ \begin{aligned} s &= S(a' + \tfrac{1}{2} \Delta a') \Delta a'' = -S(a'' + \tfrac{1}{2} \Delta a'') \Delta a', \\ s' &= S(a'' + \tfrac{1}{2} \Delta a'') \Delta a = -S(a + \tfrac{1}{2} \Delta a) \Delta a'', \\ s'' &= S(a + \tfrac{1}{2} \Delta a) \Delta a' = -S(a' + \tfrac{1}{2} \Delta a') \Delta a. \end{aligned} \right.$$

Le signe sommatoire  $S$  a rapport à trois termes qu'on déduit qui est écrit en changeant  $a$  en  $b$  et en  $c$ .

L'axe de rotation est déterminé alors aussi par

$$43) \quad . . . . . x : y : z = s : s' : s''.$$

On obtient du reste un système de relations tout à fait semblable aux formules que nous avons déduites dans le n<sup>o</sup> 4; je crois inutile de m'y arrêter et je me contenterai de donner ces relations

$$44) \quad . . \begin{cases} s = a p + b q + c r, & p = a s + a' s' + a'' s'', \\ s' = a' p + b' q + c' r, & q = b s + b' s' + b'' s'', \\ s'' = a'' p + b'' q + c'' r, & r = c s + c' s' + c'' s''. \end{cases}$$



## XXVII.

(Paris, C.-R. Acad. Sci., 98, 1884, 663—664.)

### Sur quelques applications arithmétiques de la théorie des fonctions elliptiques.

(Extrait d'une Lettre adressée à M. Hermite.)

Je viens de lire, dans les Comptes rendus, l'intéressant article de Hurwitz, qui m'a fait consulter de nouveau l'article de M. Liouville (Série, t. IV). M. Hurwitz a parfaitement raison en disant qu'une partie des résultats que j'ai donnés se déduisent des théorèmes que Liouville y donne. En effet, ces théorèmes ne sont autre chose que l'interprétation arithmétique de votre première formule

$$1 + 2^2 q^{2^2} + 3^2 q^{3^2} + \dots \\ (1 - 2q + 2q^{2^2} + 2q^{3^2} + \dots) \left[ \frac{q^1}{(1+q)^2} + \frac{q^3}{(1+q^3)^2} + \frac{q^5}{(1+q^5)^2} + \dots \right]$$

vous savez que la déduction de cette relation

$$F(4^k m) = 240 [2f(k) - 1] B(m) \quad (m \equiv 1, \text{ mod } 8)$$

on peut tirer de là, et alors votre seconde formule

$$1^2 q^{\frac{1^2}{4}} + 3^2 q^{\frac{3^2}{4}} + 5^2 q^{\frac{5^2}{4}} + \dots \\ = \left( q^{\frac{1}{4}} + q^{\frac{9}{4}} + q^{\frac{25}{4}} + \dots \right) \left[ 1 + \frac{8q^2}{(1+q^2)^2} + \frac{8q^4}{(1+q^4)^2} + \dots \right]$$

quelque théorème arithmétique équivalent) devient indispensable.

En fin de son article, M. Liouville dit lui-même que ces théorèmes ont lieu à quelques résultats curieux concernant la décomposition en cinq carrés, et il exprime son intention d'exposer cela dans un autre article; mais je ne crois pas qu'il ait publié cet article.

Quand je me suis occupé de la décomposition en sept carrés, la

première chose que j'ai tâché d'obtenir, c'étaient ces relations entre  $F_7(4m)$  et  $F_7(m)$ . J'avais mené à bonne fin cette recherche, mais je sentais encore le besoin de revoir mes raisonnements et mes calculs. Après cette revision, voici les résultats, qui ne sont guère plus compliqués que dans le cas de la décomposition en cinq carrés.

Soient  $f(k) = \frac{40 \cdot 32^k - 9}{31}$ ,  $g(k) = \frac{32^{k+1} - 1}{31}$  et  $F_7(n)$  le nombre total des décompositions de  $n$  en sept carrés, alors

$$F_7(4^k m) = f(k) F_7(m) \quad (m \equiv 1 \text{ ou } 2, \text{ mod } 4),$$

$$F_7(4^k m) = g(k) F_7(m) \quad (m \equiv 3 \text{ mod } 8),$$

$$F_7(4^k m) = \frac{28f(k) + 9}{37} F_7(m) \quad (m \equiv 7 \text{ mod } 8).$$

Il serait intéressant de déduire ces relations encore des formules elliptiques, mais je n'ai point sérieusement abordé cette question, ayant abandonné ces recherches après quelques tentatives infructueuses, et, pour le moment, d'autres travaux demandent tous mes efforts. Mais voici encore un autre résultat, bien particulier certainement, lequel conduit l'analyse des fonctions elliptiques.

Soit  $d$  un nombre parcourant les diviseurs impairs de  $n$ ,

$$\psi(n) = \sum (-1)^{\frac{1}{2}(d-1) + \frac{1}{8}(d^2-1)} = \sum \left( \frac{-2}{d} \right) \text{ et } \psi(0) = \frac{1}{2},$$

ors, dans le cas  $n \equiv 2 \pmod{4}$ , on peut exprimer la fonction  $F(n)$  de Kronecker par la formule

$$F(n) = \frac{1}{2} \sum \psi(n - 2r^2) = \sum \psi(n - 8r^2) \quad (r = 0, \pm 1, \pm 2, \dots).$$

l'aide de la méthode de M. Hurwitz, on peut tirer de là la valeur  $F(2k^2)$ , en sorte que la relation générale

$$F(np^{2k}) = [p^k + p^{k-1} + \dots + p + 1 - \left( \frac{-n}{p} \right) (p^{k-1} + \dots + p + 1)] F(n)$$

est vérifiée maintenant, dans les cas  $n = k^2$ ,  $n = 2k^2$ , à l'aide des formules elliptiques.

## XXVIII.

(Bul. Sci. math., Paris, sér. 2, 8, 1884, 175—176.)

### Sur le caractère du nombre 2 comme résidu ou non-résidu quadratique.

Soit  $p$  un nombre premier impair et considérons la suite des  
— 1 nombres

(A) . . . . . 1, 2, 3, ...,  $p - 1$ .

Tous dirons que deux nombres consécutifs  $k, k + 1$  présentent une  
variation lorsque l'un d'eux est résidu, l'autre non-résidu quadra-  
tique de  $p$ .

Cela posé, on voit facilement que le nombre total des variations  
dans la suite (A) est égal à  $\frac{p-1}{2}$ . En effet, deux nombres  $k, k + 1$ ,  
présentent une variation ou non, selon que le nombre  $r_k$  défini par

$$k + 1 \equiv k r_k \pmod{p}$$

est non-résidu ou résidu. Mais il est évident que les nombres

$$r_1, r_2, r_3, \dots, r_{p-2}$$

sont tous différents et qu'aucun d'eux n'est égal à l'unité, en sorte  
que ces nombres sont

$$2, 3, 4, \dots, p - 1,$$

en faisant abstraction de l'ordre. Le nombre des non-résidus parmi  
eux, c'est-à-dire le nombre des variations dans la suite (A), est donc  
bien égal à  $\frac{p-1}{2}$ .

Supposons maintenant  $p \equiv 1 \pmod{4}$ . Le nombre des variations dans  
la suite (A) étant pair, et le premier nombre 1 de cette suite étant

résidu, il s'ensuit que le dernier  $p-1$  ou  $-1$  est aussi résidu. Deux nombres  $k$  et  $p-k$  sont donc en même temps résidus ou non-résidus: l'où il suit que le nombre des variations dans la suite

$$B) \dots\dots\dots 1, 2, 3, \dots, \frac{p-1}{2}$$

est égal à  $\frac{p-1}{4} = n$ .

Si  $n$  est pair, c'est-à-dire  $p \equiv 1 \pmod{8}$ , le dernier nombre  $\frac{p-1}{2}$  sera donc nécessairement résidu, et partant 2 est résidu.

Si  $n$  est impair, c'est-à-dire  $p \equiv 5 \pmod{8}$ ,  $\frac{p-1}{2}$  et 2 seront non-résidus.

Soit en second lieu  $p \equiv 3 \pmod{4}$ . Le nombre des variations dans la suite (A) étant impair,  $p-1$  ou  $-1$  sera non-résidu et le nombre des variations dans la suite (B) sera égal à  $\frac{p-3}{4} = n$ .

Si  $n$  est pair, c'est-à-dire  $p \equiv 3 \pmod{8}$ ,  $\frac{p-1}{2}$  sera résidu, partant sera non-résidu.

Si  $n$  est impair, c'est-à-dire  $p \equiv 7 \pmod{8}$ ,  $\frac{p-1}{2}$  sera non-résidu et résidu quadratique de  $p$ .

---

# XXIX.

(Astr. Nachr., Kiel, 109, 1884, 145—152.)

## Quelques remarques sur l'intégration d'une équation différentielle.

1. L'équation différentielle, étudiée par M. H. Bruns dans les nos 2538, 2553 de ce Journal (voyez aussi l'article de M. Callandreau dans le n° 2547)

$$\frac{d^2x}{dt^2} + n^2 x = 2 \beta x \cos t$$

a été considérée aussi par M. F. Lindemann dans les Mathematische Annalen, Bd. XXII, p. 117 e. s. Il m'a paru intéressant de rapprocher ces deux solutions et de déduire les conclusions de M. Bruns de l'analyse de M. Lindemann.

En posant  $\cos^2 \frac{1}{2} t = u$ , on obtient

$$u(1-u) \frac{d^2x}{du^2} + \frac{1}{2}(1-2u) \frac{dx}{du} + (n^2 + 2\beta - 4\beta u)x = 0$$

les deux intégrales particulières dont se compose l'intégrale générale sont, d'après l'analyse de M. Lindemann

$$\begin{cases} C \sqrt{F(u)} e^{+iM \int \frac{du}{F(u) \sqrt{u(1-u)}}} \\ C_1 \sqrt{F(u)} e^{-iM \int \frac{du}{F(u) \sqrt{u(1-u)}}} \end{cases} \quad (i = \sqrt{-1})$$

Ici

$$F(u) = \sum_0^{\infty} c_k u^k$$

est une série, convergente pour une valeur quelconque de  $u$ .  $C$  et  $C_1$

et deux constantes arbitraires, mais la constante  $M$  est parfaitement déterminée dès qu'on connaît  $F(u)$ ; en effet, la substitution des expressions précédentes dans l'équation différentielle conduit à la relation

$$M^2 = \frac{1}{2} u (1-u) F(u) F''(u) - \frac{1}{4} u (1-u) F'(u) F'(u) + \\ + \frac{1}{4} (1-2u) F(u) F'(u) + (n^2 + 2\beta - 4\beta u) F(u) F(u).$$

On en déduit par la différentiation et division par  $F(u)$

$$u (1-u) F'''(u) + \frac{3}{2} (1-2u) F''(u) + \\ + (4n^2 + 8\beta - 1 - 16\beta u) F'(u) - 8\beta F(u) = 0.$$

A un facteur constant près, qui s'élimine de lui-même dans les expressions (2), la fonction  $F(u)$  est parfaitement déterminée par ces deux conditions: 1<sup>o</sup> de satisfaire à l'équation (5), 2<sup>o</sup> d'être holomorphe sur tout le plan.

2. En introduisant de nouveau  $t$ , les intégrales de l'équation (1) se présentent sous la forme

$$G(t) = C \sqrt{F(\cos^2 \frac{1}{2} t)} e^{+iM \int^t \frac{dt}{F(\cos^2 \frac{1}{2} t)}},$$

$$G_1(t) = C_1 \sqrt{F(\cos^2 \frac{1}{2} t)} e^{-iM \int^t \frac{dt}{F(\cos^2 \frac{1}{2} t)}}.$$

Supposons maintenant, ce qui a lieu en général, que la constante  $M$  qui est déterminée par (4), soit différente de zéro. Alors on voit que  $F(u)$  et  $F'(u)$  ne peuvent s'évanouir pour une même valeur de  $u$ , en sorte que toutes les racines de  $F(u) = 0$  sont des racines simples, et de plus les valeurs 0 et 1 ne sont point des racines de cette équation.

On en conclut que la fonction  $F(\cos^2 \frac{1}{2} t)$ , qui est aussi une fonction holomorphe de  $t$ , n'admet que des racines simples en la considérant comme fonction de  $t$ , comme nous le ferons dans la suite. Cela étant, il est facile de voir que  $G(t)$  et  $G_1(t)$  sont des fonctions périodiques de  $t$ . Supposons en effet que la variable  $t$ , en partant d'une valeur  $t_0$  décrit un contour fermé, en sorte que la valeur finale est égale à  $t_0$ . Alors, si le contour contient une seule racine  $a$  de

$(\cos^2 \frac{1}{2} t) = 0$ , les valeurs initiales et finales de  $\sqrt{F(\cos^2 \frac{1}{2} t)}$  sont de signe contraire. Mais l'intégrale  $\int^t \frac{dt}{F(\cos^2 \frac{1}{2} t)}$  aura éprouvé un accroissement égal à

$$\frac{\pm 2i\pi}{F'(a)\sqrt{a(1-a)}}$$

mais, d'après (4) on a

$$2iM = \pm F'(a)\sqrt{a(1-a)}$$

l'expression exponentielle  $e^{\pm iM \int^t \frac{dt}{F(\cos^2 \frac{1}{2} t)}}$  sera donc multipliée par le facteur  $e^{\pm i\pi} = -1$ , en sorte que la valeur finale de  $G(t)$  coïncide avec la valeur initiale. La même chose a lieu quand le contour enfermerait plusieurs racines;  $G(t)$  et  $G_1(t)$  sont donc bien des fonctions uniformes de  $t$ , de plus elles ne deviennent jamais infinies.

En étudiant d'une manière analogue la variation qu'éprouve la fonction  $G(t)$ , lorsque la variable croît d'une valeur  $t$  à  $t + 2\pi$ , on arrive au résultat suivant:

Considérons l'intégrale:  $\int_0^{2\pi} \frac{dt}{F(\cos^2 \frac{1}{2} t)}$ , le chemin de l'intégration peut être choisi d'une manière arbitraire, seulement il ne doit passer par aucune racine de  $F(\cos^2 \frac{1}{2} t) = 0$ . Supposons que dans l'expression  $\sqrt{F(\cos^2 \frac{1}{2} t)}$  on fait varier la variable  $t$  de 0 à  $2\pi$  en passant par les mêmes valeurs que dans l'intégrale. Alors les valeurs initiales et finales de  $\sqrt{F(\cos^2 \frac{1}{2} t)}$  se distingueront par le facteur  $(-1)^r$ ,  $r$  étant égale à 0 ou à 1. Posons

$$\mu = (-1)^r e^{iM \int_0^{2\pi} \frac{dt}{F(\cos^2 \frac{1}{2} t)}}$$

lors

$$G(t + 2\pi) = \mu G(t),$$

$$G_1(t + 2\pi) = \frac{1}{\mu} G_1(t).$$

La constante  $\mu$  est indépendante du chemin de l'intégration qu'on choisit. En déterminant donc  $m$  par

$$\mu = e^{2i\pi m}$$

est-à-dire

$$\dots \dots \dots m = \frac{M}{2\pi} \int_0^{2\pi} \frac{dt}{F(\cos^2 \frac{1}{2}t)} + \frac{r}{2}$$

posant

$$G(t) = e^{+imt} H(t),$$

$$G_1(t) = e^{-imt} H_1(t),$$

aura  $H(t + 2\pi) = H(t)$ ,  $H_1(t + 2\pi) = H_1(t)$ , et d'après un théorème connu, on pourra donc développer ces fonctions de la manière suivante

$$H(t) = \sum_{k=-\infty}^{+\infty} m_k e^{ik t},$$

$$H_1(t) = \sum_{k=-\infty}^{+\infty} n_k e^{ik t},$$

les séries étant convergentes pour une valeur quelconque de  $t$ .

Nous avons retrouvé ainsi le résultat de M. Bruns, on voit de plus que la constante  $m$ , déterminée par (6), a la même signification que dans le mémoire de M. Bruns.

Comme la détermination de cette constante  $m$  est la principale difficulté qu'on rencontre dans l'application numérique, nous allons donner un moyen facile pour obtenir l'expression de la fonction  $G(u)$  qui figure dans (6). En effet, les moyens proposés par M. Lindemann pour déterminer  $F(u)$ , quoique irréprochables au point de vue théorique, ne sont pas propres pour le calcul

3. La substitution de la série  $\sum_0^{\infty} c_k u^k$  dans l'équation différentielle

) conduit à une relation récurrente, que nous écrivons ainsi

$$\dots \dots \dots v_{k+1} c_{k+2} = u_k c_{k+1} + c_k,$$



$$\left\{ \begin{aligned} u_k &= \frac{(k+1)[(k+1)^2 - 4n^2 - 8\beta]}{8\beta(2k+1)}, \\ v_k &= \frac{k(k+1)(2k+1)}{16\beta(2k-1)}. \end{aligned} \right.$$

Il semble donc qu'on peut choisir arbitrairement  $c_0$  et  $c_1$ , pour calculer successivement  $c_2, c_3, \dots$ . Mais cela n'est pas, car en agissant ainsi, la série  $\sum c_k u^k$  ne serait pas convergente pour une valeur quelconque de  $u$ . Il faut au contraire déterminer le rapport  $c_1 : c_0$  par cette condition que la série converge toujours. Supposons  $\beta$  différent de zéro (pour  $\beta = 0$  l'équation (1) s'intègre immédiatement) on voit que  $u_k, v_k$  deviennent infiniment grand avec  $k$ , mais leur rapport approche de l'unité. Pour une valeur assez grande de  $k$  la fraction continue

$$u_k + v_{k+1} : u_{k+1} + v_{k+2} : u_{k+2} + v_{k+3} : \dots$$

sera donc convergente, et l'on calcule facilement sa valeur numérique, qui sera peu différente de  $u_k$  lorsque  $k$  est grand.

Cela étant, donnons à  $c_k$  une valeur arbitraire différente de zéro et calculons  $c_{k+1}$  par la formule

$$-\frac{c_k}{c_{k+1}} = u_k + v_{k+1} : u_{k+1} + v_{k+2} : \dots$$

Connaissant maintenant  $c_k$  et  $c_{k+1}$  on peut calculer tous les autres coefficients à l'aide de (7). Lorsqu'aucun des coefficients  $c_0, c_1, \dots, c_{k-1}$  évanouit, cela revient à la même chose que d'appliquer la formule (7) pour  $k=0, 1, 2, \dots$ .

Il est évident d'abord, qu'en agissant ainsi la série  $\sum c_k u^k$  satisfait à l'équation différentielle (5); et en second lieu, pour une valeur assez grande de  $k$  on a à peu près  $\frac{c_k}{c_{k+1}} = -u_k$ , en sorte que la série converge pour une valeur quelconque de  $u$ .

Ayant obtenu la fonction  $F(u)$ , on trouvera  $M$  par l'équation (4), par exemple en posant  $u=0$

$$M^2 = \frac{1}{4} c_0 c_1 + (n^2 + 2\beta) c_0 c_0.$$

Si la valeur de  $M$  qu'on en déduit est réelle (nous supposons maintenant  $n^2$  et  $\beta$  réels), la fonction  $F(u)$  ne peut s'évanouir pour une valeur réelle de  $u$  comprise entre 0 et 1; en effet, lorsque  $F(u)=0$ , on a

$$M^2 = -\frac{1}{4} u (1-u) F'(u) F'(u).$$

Dans ce cas on peut choisir dans (6) un chemin d'intégration rectiligne et  $r=0$ . En appliquant une quadrature mécanique pour le calcul numérique on pourra donc calculer  $m$  à l'aide de l'expression

$$(11) \quad m = \frac{M}{s} \sum_{k=1}^s \frac{1}{F\left(\cos^2 \frac{(2k-1)\pi}{4s}\right)}.$$

4. Il résulte de l'analyse de M. Bruns que la valeur de  $m$  ne change point quand on remplace  $\beta$  par  $-\beta$ . On peut le vérifier aussi à l'aide des formules obtenues. L'équation (5) ne changeant point lorsqu'on remplace simultanément  $\beta$  par  $-\beta$  et  $u$  par  $1-u$ , on en conclut

$$(12) \quad F(-\beta, u) = A F(\beta, 1-u),$$

$A$  étant une constante. Nous écrivons maintenant  $F(\beta, u)$  au lieu de  $F(u)$  pour mettre en évidence la constante  $\beta$ . Soit  $M'$  la valeur de  $M$ , quand  $\beta$  est remplacé par  $-\beta$ , alors

$$M^2 = \frac{1}{4} F(\beta, 0) F'(\beta, 0) + (n^2 + 2\beta) F(\beta, 0) F(\beta, 0)$$

et posant  $u=1$  dans (4) après avoir changé  $\beta$  en  $-\beta$

$$M'^2 = -\frac{1}{4} F(-\beta, 1) F'(-\beta, 1) + (n^2 + 2\beta) F(-\beta, 1) F(-\beta, 1).$$

En posant  $u=1$  dans l'équation (12) et dans celle qu'on en déduit par la différentiation, on voit que

$$M'^2 = A^2 M^2$$

et comme le signe est indifférent,  $M' = A M$ . Mais on a

$$m = \frac{M}{2\pi} \int_0^{2\pi} \frac{dt}{F(\beta, \cos^2 \frac{1}{2} t)} + \frac{r}{2}$$

$$m' = \frac{M'}{2\pi} \int_0^{2\pi} \frac{dt}{F(-\beta, \cos^2 \frac{1}{2} t)} + \frac{r'}{2},$$

désignant par  $m'$  la valeur de  $m$  après le changement de  $\beta$  en  $-\beta$ .  
 se rapportant à la signification de  $r$  et  $r'$ , on voit facilement que  
 relation (12) donne  $r = r'$ , et l'on aura  $m = m'$  comme l'a trouvé  
 Bruns. Au reste il va sans dire que la constante  $m$  n'étant pas  
 erement déterminée, on peut toujours remplacer  $m$  par  $m + k$ ,  
 ant un nombre entier, et changer encore le signe de  $m$ . Dans  
 pression (6) cette double indétermination est indiquée d'abord  
 e que le signe de  $M$ , n'est pas déterminé, et en second lieu  
 e que le chemin de l'intégration reste arbitraire.  
 ur compléter cette étude, il faudrait discuter le cas  $M = 0$ . Mais  
 ne cette discussion devient un peu longue parce qu'il y a plu-  
 s cas à distinguer et qu'elle est de peu d'importance pour l'ap-  
 tion, je n'entrerai point dans cette discussion.

Quand  $\beta = 0$ , la fonction  $F(u)$  se réduit à une constante, et  
 peut, pour une valeur suffisamment petite de  $\beta$ , développer  $F(u)$   
 ant les puissances croissantes de  $\beta$ . Il est aisé d'obtenir ce dé-  
 ppelement. En effet, en posant  $c_0 = 1$ , on voit facilement à l'aide  
 fractions continues qui expriment les rapports  $c_0 : c_1$ ,  $c_1 : c_2$  etc.  
 le développement suivant les puissances de  $\beta$  donnera

$$c_1 = p_1 \beta + p_2 \beta^2 + p_3 \beta^3 + \dots,$$

$$c_2 = q_2 \beta^2 + q_3 \beta^3 + \dots,$$

$$c_3 = r_3 \beta^3 + \dots,$$

en sorte qu'en général  $c_k$  commence par un terme avec  $\beta^k$ . On  
 ra calculer encore facilement de proche en proche les coefficients  
 $p_1, \dots, q_2, \dots$  qui dépendent seulement de  $n^2$ . Ce sont des fonc-  
 tionnelles de  $n^2$ , dont les dénominateurs renferment seulement  
 facteurs de la forme  $4n^2 - k^2$ ,  $k$  étant un nombre entier. On  
 par conséquent

$$F(u) = 1 + L_1 \beta + L_2 \beta^2 + L_3 \beta^3 + \dots,$$

$$L_1 = p_1 u,$$

$$L_2 = p_2 u + q_2 u^2,$$

$$L_3 = p_3 u + q_3 u^2 + r_3 u^3,$$

etc.

Nous pouvons obtenir maintenant sans difficulté le développement de  $m$  suivant les puissances de  $\beta$ , développement dont M. Bruns a calculé les premiers termes par un procédé bien différent. En effet, la formule (6) devient dans le cas actuel que  $\beta$  est suffisamment petit

$$(3) \quad m = \frac{M}{2\pi} \int_0^{2\pi} \frac{dt}{F(\cos \frac{1}{2} t)}$$

La formule (10) donne à cause de  $c_0 = 1$

$$M^2 = n^2 + 2\beta + \frac{1}{4}c_1.$$

Il suffit donc de développer  $M$  et  $1:F(u)$  suivant les puissances de  $\beta$ , et de substituer dans la formule (13) pour obtenir le développement cherché de  $m$ . Comme nous le savons ce développement doit renfermer seulement les puissances paires de  $\beta$ , c'est ce qu'on ne voit pas à priori par le calcul indiqué. Il vaut donc mieux de diriger le calcul d'une manière légèrement différente.

Déterminons la constante arbitraire que renferme  $F(u)$  de manière que  $F(\frac{1}{2}) = 1$  et posons

$$(4) \quad F\left(\frac{1}{2} + v\right) = c_0 + c_1 v + c_2 v^2 + c_3 v^3 + \dots$$

où  $c_0 = 1$ . La comparaison avec le développement  $F(u) = \sum c_k u^k$  fait voir que le développement de  $c_k$  suivant les puissances de  $\beta$  commence par un terme avec  $\beta^k$ . En outre la formule (12) fait voir maintenant que la série  $\sum c_k v^k$  doit rester la même en changeant la fois  $v$  en  $-v$ , et  $\beta$  en  $-\beta$ , en sorte que le développement de  $c_k$  contiendra seulement des termes en  $\beta^k, \beta^{k+2}, \beta^{k+4}, \dots$ . En posant donc

$$F\left(\frac{1}{2} + v\right) = N_0 + N_1 \beta + N_2 \beta^2 + N_3 \beta^3 + \dots$$

$N_k$  sera un polynôme en  $v$  qui contiendra seulement des termes en  $v^k, v^{k-2}, v^{k-4}, \dots$  et qui ne renferme point de terme sans  $v$ . On trouve

$$\begin{aligned}
&= 1 \\
&= \frac{4}{4n^2 - 1} v \\
&= \frac{24}{(4n^2 - 1)(4n^2 - 4)} v^2 \\
&= \frac{160}{(4n^2 - 1)(4n^2 - 4)(4n^2 - 9)} \left[ v^3 - \frac{6}{4n^2 - 1} v \right] \\
&= \frac{1120}{(4n^2 - 1)(4n^2 - 4)(4n^2 - 9)(4n^2 - 16)} \left[ v^4 - \frac{60}{7} \cdot \frac{8n^2 - 11}{(4n^2 - 1)(4n^2 - 4)} v^2 \right].
\end{aligned}$$

En général, lorsqu'on connaît les coefficients  $\alpha, \beta, \gamma, \dots$  du polynôme

$$N_{k-1} = \alpha v^{k-1} - \beta v^{k-3} + \gamma v^{k-5} - \delta v^{k-7} + \dots$$

pourra calculer ceux du polynôme  $N_k$

$$N_k = \alpha_1 v^k - \beta_1 v^{k-2} + \gamma_1 v^{k-4} - \delta v^{k-6} + \dots$$

à l'aide des formules suivantes

$$\begin{aligned}
k[4n^2 - k^2] \alpha_1 &= 4(2k - 1) \alpha, \\
(k - 2)[4n^2 - (k - 2)^2] \beta_1 - k(k - 1)(k - 2) \alpha_1 &= 4(2k - 5) \beta, \\
(k - 4)[4n^2 - (k - 4)^2] \gamma_1 - (k - 2)(k - 3)(k - 4) \beta_1 &= 4(2k - 9) \gamma, \\
(k - 6)[4n^2 - (k - 6)^2] \delta_1 - (k - 4)(k - 5)(k - 6) \gamma_1 &= 4(2k - 13) \delta,
\end{aligned}$$

et la loi est évidente. C'est ce qu'on trouve sans difficulté à l'aide de l'équation différentielle à laquelle satisfait la fonction  $F(u)$ .

Le développement de  $F\left(\frac{1+v}{2}\right)$  étant obtenu ainsi, on en déduit

$$1 : F\left(\frac{1+v}{2}\right) = 1 - N_1 \beta + (N_1^2 - N_2) \beta^2 - (N_1^3 - 2N_1 N_2 + N_3) \beta^3 + \dots,$$

$$\int_0^{2\pi} \frac{dt}{F(\cos^2 \frac{1}{2} t)} = 1 + (N_1^2 - N_2) \beta^2 + (N_1^4 - 3N_1^2 N_2 + 2N_1 N_3 + N_2^2 - N_4) \beta^4 + \dots,$$

la condition qu'on remplace dans le second membre  $v^{2k}$  par  $\frac{1 \cdot 3 \cdot 5 \dots (2k - 1)}{2 \cdot 4 \cdot 6 \dots (2k)}$ , c'est-à-dire par  $\frac{1}{2\pi} \int_0^{2\pi} \cos^{2k} t dt$ . Quant à la valeur

$M$ , il faut la déduire de

$$M^2 = n^2 + e_2 - \frac{1}{4} e_1 e_1,$$

et  $e_2$  étant les coefficients de  $v$  et de  $v^2$  dans

$$N_0 + N_1 \beta + N_2 \beta^2 + \dots$$

on voit que le développement de  $M$  et par conséquent aussi celui de  $m$  contient seulement les puissances paires de  $\beta$ . En effectuant les calculs indiqués j'ai retrouvé les valeurs de  $m_1, m_2$  données par  $M. Bruns$ , dans le développement  $m = n + m_1 \beta^2 + m_2 \beta^4 + \dots$ . Rappelons ici qu'il ne convient pas de calculer  $m$  par cette formule, mais on peut en déduire cet autre

$$\cos 2 \pi m = \cos 2 \pi n + 2 \pi^2 \sum_1^{\infty} f_k \beta^{2k}$$

qui converge pour une valeur quelconque de  $m$  comme l'a démontré  $M. Bruns$ .

6. Nous avons vu comment on peut calculer les coefficients  $c_k$  de la série  $F(u) = \sum c_k u^k$ . Mais on peut obtenir encore un peu plus complètement les coefficients de la série

$$F(\cos^2 \frac{1}{2} t) = \frac{1}{2} g_0 + g_1 \cos t + g_2 \cos 2 t + g_3 \cos 3 t + \dots$$

à l'aide des formules

$$v_{k+1} g_{k+2} = -\mu_k g_{k+1} - g_k,$$

$$\left\{ \begin{array}{l} \mu_k = \frac{(k+1)[(k+1)^2 - 4n^2]}{2\beta(2k+1)} \\ v_k = \frac{2k+1}{2k-1} \end{array} \right.$$

$$-\frac{g_k}{g_{k+1}} = \mu_k - v_{k+1} : \mu_{k+1} - v_{k+2} : \mu_{k+2} - \dots$$

Les coefficients  $g_k$  décroissent, comme on le voit, encore plus rapidement que les  $c_k$ , mais par contre le calcul de  $M$  n'est pas aussi simple, il faut se servir des formules suivantes

$$M^2 = \frac{1}{4} F(0) F'(0) + (n^2 + 2\beta) F(0) F(0),$$

$$M^2 = -\frac{1}{4} F(1) F'(1) + (n^2 - 2\beta) F(1) F(1),$$

$$F'(0) = 2 [g_1 - 2^2 g_2 + 3^2 g_3 - 4^2 g_4 + 5^2 g_5 - \dots],$$

$$F'(1) = 2 [g_1 + 2^2 g_2 + 3^2 g_3 + 4^2 g_4 + 5^2 g_5 + \dots].$$

on pourrait encore calculer directement les coefficients  $e_k$  du développement de  $F\left(\frac{1+v}{2}\right)$  suivant les puissances de  $v$ , elles sont par la relation

$$4\beta(2k+1)e_k = -(k+1)[(k+1)^2 - 4n^2]e_{k+1} + (k+1)(k+2)(k+3)e_{k+3}.$$

On ne peut pas exprimer directement par une fraction continue l'apport de deux coefficients consécutifs, mais cela est assez incommode pour le calcul numérique. On peut démontrer rigoureusement qu'on peut calculer  $e_0, e_1, e_2, \dots$  avec une approximation aussi grande qu'on veut par le procédé suivant. Pour une valeur suffisamment grande de l'indice  $r$  on prendra  $e_{r+1} = 0, e_{r+2} = 0$  et  $e_r$  égale à une quantité arbitraire différente de zéro. Il faut ensuite calculer  $e_{r-1}, e_{r-2}, \dots, e_0$  à l'aide de la relation (19). Quelques applications numériques m'ont fait voir qu'au point de vue de la commodité il n'y a pas une grande différence entre cette manière et celle dans laquelle on se sert des formules (15) à (18). Mais ces méthodes semblent présenter un léger avantage sur le calcul des coefficients  $e_k$ . Quand on aura calculé les  $e_k$  il faudra calculer  $M$  par

$$M^2 = e_0 e_2 - \frac{1}{4} e_1 e_1 + n^2 e_0 e_0.$$

Dans ce qui précède j'ai dit que la fonction  $F(u)$  renferme seulement un facteur constant arbitraire. Cela est vrai en général, mais quand  $\beta = 0$  et qu'en même temps  $n$  est la moitié d'un nombre entier, l'expression générale de  $F(u)$  est un polynôme en  $u$  renfermant des constantes arbitraires; on a en effet dans ce cas

$$F(\cos^2 \frac{1}{2} t) = A \cos^2 n t + B \sin^2 n t.$$

# XXX.

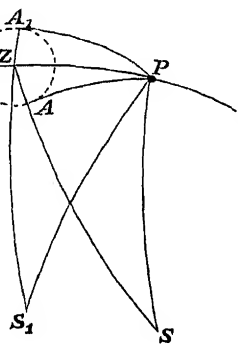
(Astr. Nachr., Kiel, 110, 1884, 7—8.)

## Note sur le problème du plus court crépuscule.

A l'occasion des articles de M. Zelbr dans les nos 2575, 2602 j'ai fait la remarque que la solution de ce problème ne devient guère plus compliquée en tenant compte de la réfraction et du diamètre du soleil. Mais cela résulte déjà de l'article du Dr. Stoll cité par M. Zelbr dans le n° 2602, article qui contient en effet la solution analytique complète du problème.

Supposons que le commencement et la fin du crépuscule aient lieu lorsque la dépression du soleil sous l'horizon est égale respectivement à  $c(=18^\circ)$  et à  $d$ . Soient: Z le zénith, P le pôle, S et  $S_1$  les positions du soleil au commencement et à la fin du crépuscule. Traçons les arcs de grand cercle  $PS=PS_1=90^\circ-\delta$ ,  $ZS=90^\circ+c$ ,  $ZS_1=90^\circ+d$ .

La variation de l'angle  $SPS_1$  devant être égale à zéro pour une variation infiniment petite de la déclinaison du soleil, on en conclut facilement qu'on doit avoir  $\angle PSZ = \angle PS_1Z$ . (Voir p. e. *Landes, Astronomie*, II, p. 557, 3<sup>ième</sup> édit.) Prenons maintenant  $A = \frac{1}{2}(c-d)$  et prolongeons l'arc  $S_1Z$  jusqu'en  $A_1$  en sorte que  $A_1Z = ZA = \frac{1}{2}(c-d)$ , enfin traçons les arcs de grand cercle  $PA, PA_1$ . Comme on a  $SA = S_1A_1 = 90^\circ + \frac{1}{2}(c+d)$  les triangles  $PSA, PS_1A_1$  sont égaux et  $PA = PA_1$ ,  $\angle SAP = \angle S_1A_1P$ . Mais de l'égalité  $PA = PA_1$  on conclut que les triangles  $PZA, PZA_1$  sont égaux, donc:  $\angle S_1A_1P = \angle ZAP = \angle SAP$ . Les angles  $SAP, S_1A_1P$  sont





des angles droits et l'on obtient A et A<sub>1</sub> en menant les arcs PA<sub>1</sub> tangents au petit cercle décrit de Z avec un rayon égal (c - d). Les azimuts PZS, PZS<sub>1</sub> sont supplémentaires. On voit plus que l'angle SPS<sub>1</sub> qui mesure la durée du plus court crépuscule est égale à l'angle APA<sub>1</sub>.

Les triangles rectangles PAZ, PAS donnent

$$\cos PA = \frac{\sin \varphi}{\cos \frac{1}{2}(c - d)},$$

$$\sin \delta = \cos PA \cos SA = -\cos PA \sin \frac{1}{2}(c + d)$$

c

$$\sin \delta = -\sin \varphi \frac{\sin \frac{1}{2}(c + d)}{\cos \frac{1}{2}(c - d)}.$$

En posant  $\angle ZPS = t$ ,  $\angle ZPS_1 = t_1$  on a  $\angle APZ = \frac{1}{2}(t - t_1)$ ,  $\angle S_1PA_1 = \frac{1}{2}(t + t_1)$ , donc

$$\sin \frac{1}{2}(t - t_1) = \frac{\sin \frac{1}{2}(c - d)}{\cos \varphi},$$

$$\sin \frac{1}{2}(t + t_1) = \frac{\cos \frac{1}{2}(c + d)}{\cos \delta}.$$

Enfin l'azimut du soleil au commencement et à la fin du crépuscule déterminent à l'aide de

$$\cos PZS = -\cos PZS_1 = \operatorname{tg} \varphi \operatorname{tg} \frac{1}{2}(c - d).$$

En traitant le problème par l'analyse on est conduit à une seconde solution qui se déduit de la première en changeant c en  $180^\circ - c$ . Elle est réelle seulement dans le cas qu'il est possible de mener par P un grand cercle tangent au petit cercle décrit de Z avec un rayon égal à  $90^\circ - \frac{1}{2}(c + d)$ , c'est-à-dire lorsque  $\varphi$  est inférieur à  $\frac{1}{2}(c + d)$ . Je crois inutile d'insister sur la signification de cette seconde solution.

## XXXI.

(Ann. Sci. Éc. norm., Paris, sér. 3, 1, 1884, 409—426.)

### Quelques recherches sur la théorie des quadratures dites mécaniques.

#### *Introduction.*

Les formules d'approximation qui servent à calculer la valeur numérique d'une intégrale définie ont été l'objet d'une étude d'ensemble, de la part de M. Radau, dans le Tome VI (3<sup>e</sup> série) du Journal de mathématiques pures et appliquées.

L'auteur y a réuni à peu près tout ce qui est connu sur ce sujet, en donnant les constantes dont on peut avoir besoin dans l'application, il a encore augmenté l'utilité de son travail.

Les recherches suivantes ont été dirigées par une autre idée. En plaçant au point de vue le plus général, mon but a été d'étudier la question de savoir si ces formules permettent d'atteindre une approximation indéfinie.

Jusqu'à présent, il semble que cette étude n'ait pas encore été abordée. On a toujours supposé que la fonction dont il s'agit est développable en série suivant les puissances croissantes de la variable. Or, comme on le verra, ces quadratures où, à l'exemple de Gauss, les abscisses sont déterminées de manière à atteindre le plus haut degré de précision, présentent des circonstances particulières, qui ont pour conséquence qu'elles sont applicables dans des cas bien plus étendus. Par exemple, la quadrature de Gauss elle-même donne une approximation indéfinie pour toute fonction intégrable. Dans l'expo-

n de la théorie générale de cette quadrature mécanique, j'ai  
runté bien des choses au Traité des fonctions sphériques (deuxième  
on) de M. Heine, et les n<sup>os</sup> 1, 2, 4 ne contiennent rien d'essen-  
qu'on ne trouve dans ce traité.

*Détermination d'un polynôme qui satisfait à certaines conditions.*  
 $f(x)$  une fonction donnée, qui ne dévient pas négative, quand  
end les valeurs  $a$ ,  $b$  et toutes les valeurs intermédiaires, et inté-  
le dans cet intervalle, en sorte que  $\int_a^b f(x) dx$  ait un sens deter-  
é. Il n'est pas nécessaire que  $f(x)$  reste toujours finie; mais nous  
posons finies les limites  $a$  et  $b$ , bien que quelques-uns des résultats  
quels nous arriverons restent applicables dans le cas contraire.  
nfin, pour éviter certaines discussions qui n'auraient guère d'uti-  
nous ferons encore la restriction suivante: nous supposerons  
l existe un intervalle  $(A, B)$  appartenant à l'intervalle plus étendu  
 $(a, b)$  tel que, lorsque  $x$  est situé dans  $(A, B)$ ,  $f(x)$  reste constamment  
érieure à une quantité positive  $\varepsilon$ , d'ailleurs tout à fait arbitraire,  
me l'intervalle  $(A, B)$ .

Grâce à cette dernière restriction, la valeur de  $\int_a^b f(x) dx$  sera donc  
itive et différente de zéro, et nous avons écarté aussi le cas sans  
rêt où  $f(x)$  serait constamment égale à zéro dans l'intervalle  $(a, b)$ .  
ela posé, nous commençons par déterminer un polynôme  $P(x)$   
a degré donné  $n$ ,

$$P(x) = x^n + a_1 x^{n-1} + a_2 x^{n-2} + \dots + a_{n-1} x + a_n,$$

les conditions

$$\int_a^b f(x) P(x) x^k dx = 0 \quad (k = 0, 1, 2, \dots, n-1).$$

es conditions donnent lieu aux équations linéaires suivantes, qui  
rent à déterminer les inconnues  $a_1, a_2, \dots, a_n$ :

$$\begin{cases} \int_a^b f(x) x^{n+k} dx + a_1 \int_a^b f(x) x^{n+k-1} dx \\ \quad + a_2 \int_a^b f(x) x^{n+k-2} dx + \dots + a_n \int_a^b f(x) x^k dx = 0. \end{cases}$$

Le problème est donc déterminé en général, et les inconnues  $a_1, a_2, \dots, a_n$  dépendent rationnellement des  $2n$  constantes  $\int_a^b f(x) x^k dx$ , où  $k=0, 1, 2, \dots, 2n-1$ . Mais il importe de faire voir qu'en résolvant ces équations linéaires, aucune impossibilité ni indétermination ne sauraient se présenter.

Remarquons pour cela que le déterminant  $\Delta$  du système (2) est composé d'une série de termes, dont chacun est un produit de  $n$  intégrales de la forme  $\int_a^b f(x) x^k dx$ . En écrivant un tel produit sous la forme d'une intégrale multiple d'ordre  $n$ , on arrive à l'expression suivante de  $\Delta$

$$\Delta = \int_a^b \int_a^b \dots \int_a^b f(x_1) f(x_2) \dots f(x_n) \\ \times \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ x_2 & x_2^2 & x_2^3 & \dots & x_2^n \\ x_3^2 & x_3^3 & x_3^4 & \dots & x_3^{n+1} \\ \dots & \dots & \dots & \dots & \dots \\ x_n^{n-1} & x_n^n & x_n^{n+1} & \dots & x_n^{2n-2} \end{vmatrix} dx_1 dx_2 \dots dx_n$$

ou bien

$$\Delta = \int_a^b \int_a^b \dots \int_a^b f(x_1) f(x_2) \dots f(x_n) x_2^2 x_3^3 \dots x_n^{n-1} \Pi dx_1 dx_2 \dots dx_n,$$

où l'on a

$$\Pi = \begin{vmatrix} 1 & x_1 & x_1^2 & \dots & x_1^{n-1} \\ 1 & x_2 & x_2^2 & \dots & x_2^{n-1} \\ 1 & x_3 & x_3^2 & \dots & x_3^{n-1} \\ \dots & \dots & \dots & \dots & \dots \\ 1 & x_n & x_n^2 & \dots & x_n^{n-1} \end{vmatrix}.$$

La notation des variables étant indifférente, on peut, dans cette expression, permuter de toutes les manières les indices  $1, 2, \dots, n$ . Par une permutation quelconque  $\Pi$  ne change pas ou change seulement de signe, et, en ajoutant toutes les équations qu'on obtient, on aura

$$\Sigma \pm x_2^2 x_3^3 \dots x_n^{n-1} = \Pi;$$

$$1. 2. 3 \dots n \Delta = \int_a^b \int_a^b \dots \int_a^b f(x_1) f(x_2) \dots f(x_n) (\Pi)^2 dx_1 dx_2 \dots dx_n.$$

Après les conditions que nous avons imposées à  $f(x)$ , il est évident que  $\Delta$  a une valeur positive, différente de zéro.

Le polynôme cherché  $P(x)$  existe donc pour toute valeur de  $n$ , et nous désignerons ces polynômes, pour  $n = 1, 2, 3, \dots$ , par  $P_1(x), P_2(x), P_3(x), \dots$ .

*Propriétés des polynômes  $P(x)$ .* — La propriété principale du polynôme  $P_n(x)$  consiste en ce que l'on a

$$\int_a^b f(x) P_n(x) (a x^{n-1} + \beta x^{n-2} + \dots + \lambda x + \mu) dx = 0.$$

Ceci est une conséquence immédiate des équations (1) qui ont servi à déterminer  $P_n(x)$ .

Si les indices  $m$  et  $n$  étant différents, on a donc aussi

$$\int_a^b f(x) P_m(x) P_n(x) dx = 0.$$

Avec l'aide d'un raisonnement dû à Legendre, nous pouvons maintenant énoncer la proposition suivante :

Les racines de l'équation  $P_n(x) = 0$  sont réelles, inégales et comprises entre  $a$  et  $b$  en excluant les limites.

En effet, désignons par  $x_1, x_2, \dots, x_k$  les racines réelles comprises entre  $a$  et  $b$ . Le nombre de ces racines est au moins égal à 1, parce que, à cause de l'équation

$$\int_a^b f(x) P_n(x) dx = 0,$$

il doit changer de signe dans l'intervalle  $(a, b)$ .

En posant

$$P_n(x) = (x - x_1)(x - x_2) \dots (x - x_k) Q(x),$$

le polynôme  $Q(x)$  ne changera point de signe dans l'intervalle  $(a, b)$ .

r, si  $Q(x)$  n'était pas simplement égal à l'unité,

$$(x - x_1)(x - x_2) \dots (x - x_k)$$

et au plus du degré  $n - 1$ , et l'on aurait, d'après (4),

$$\int_a^b f(x) P_n(x) (x - x_1)(x - x_2) \dots (x - x_k) dx = 0,$$

qui est évidemment impossible, parce que l'intégrale a une valeur positive.

Toutes les racines de  $P_n(x) = 0$  sont donc comprises dans l'intervalle  $(a, b)$ , mais il ne saurait y avoir deux racines égales entre elles. En effet, supposons

$$P_n(x) = (x - x_1)^2 R(x),$$

étant un polynôme du degré  $n - 2$ ; on devra avoir

$$\int_a^b f(x) P_n(x) R(x) dx = 0,$$

ce qui est impossible.

*Relations entre les polynômes  $P(x)$ .* — Le polynôme  $Q(x)$  du degré  $n$ , le plus général qui satisfait aux conditions (1),

$$\int_a^b f(x) Q(x) x^k dx = 0 \quad (k = 0, 1, 2, \dots, n - 1),$$

se distingue de  $P_n(x)$  que par un facteur constant.

En effet, tout polynôme  $Q(x)$  du degré  $n$  peut se mettre sous la forme

$$Q(x) = a_0 P_n(x) + \dots + a_k P_{n-k}(x) + \dots + a_{n-1} P_1(x) + a_n.$$

Or, en multipliant par  $P_{n-k}(x) f(x) dx$  et intégrant entre les limites  $a, b$ , on trouve, à l'aide de (5),

$$0 = a_k \int_a^b f(x) [P_{n-k}(x)]^2 dx \quad (k = 1, 2, 3, \dots, n),$$

c'est-à-dire  $a_k = 0$ .

considérons maintenant l'expression

$$R(x) = P_n(x) - x P_{n-1}(x) + A P_{n-1}(x),$$

où  $A$  est une constante quelconque. Ce polynôme satisfait évidemment les conditions

$$\int_a^b f(x) R(x) x^k dx = 0 \quad (k = 0, 1, 2, \dots, n-3).$$

On peut choisir  $A$  de manière que  $R(x)$  soit du degré  $n-2$ ; cela, il suffit que  $x - A$  soit le quotient qu'on obtient en divisant  $P_n(x)$  par  $P_{n-1}(x)$ .

Après la remarque que nous venons de faire,  $R(x)$ , pour cette valeur particulière de  $A$ , ne différera que par un facteur constant de  $P_{n-2}(x)$ , en sorte que nous avons une relation de cette forme

$$P_n(x) = (x - a_{n-1}) P_{n-1}(x) - \lambda_{n-1} P_{n-2}(x)$$

$$P_1(x) = x - a_0,$$

$$P_2(x) = (x - a_1) P_1(x) - \lambda_1.$$

On peut arriver facilement à des expressions élégantes des coefficients  $a_k, \lambda_k$ . L'équation

$$P_{k+1}(x) = (x - a_k) P_k(x) - \lambda_k P_{k-1}(x)$$

est, en effet, en multipliant par  $P_k(x) f(x) dx$  et intégrant de  $x = a$  à  $x = b$ ,

$$a_k = \frac{\int_a^b x P_k(x) P_k(x) f(x) dx}{\int_a^b P_k(x) P_k(x) f(x) dx}.$$

En multipliant la même équation par  $P_{k-1}(x) f(x) dx$  et intégrant de  $x = a$  à  $x = b$ , on obtient

$$\lambda_k = \frac{\int_a^b P_k(x) P_k(x) f(x) dx}{\int_a^b P_{k-1}(x) P_{k-1}(x) f(x) dx},$$

en remarquant que  $x P_{k-1}(x) = P_k(x) +$  un polynôme de degré  $k-1$ .

On voit que  $a_k$  reste compris entre  $a$  et  $b$ , tandis que  $\lambda_k$  est toujours positif.

Les relations (6), (7) et (8) permettent de calculer de proche en proche tous les polynômes  $P_1(x)$ ,  $P_2(x)$ , .... On a d'abord

$$a_0 = \int_a^b x f(x) dx : \int_a^b f(x) dx,$$

qui fait connaître  $P_1(x)$ . Les formules (7) et (8) donnent alors  $a_1$ , ce qui fait connaître  $P_2(x)$ , ....

Mais les relations (6) conduisent encore à une autre conséquence, à compléter la proposition démontrée sur les racines de l'équation  $P_1(x) = 0$ .

Substituons la valeur  $x = a_0$ , racine de  $P_1(x) = 0$  dans

$$P_2(x) = (x - a_1) P_1(x) - \lambda_1,$$

on vient

$$P_2(a_0) = -\lambda_1,$$

quantité négative par conséquent. L'équation  $P_2(x) = 0$  a donc ses racines  $\beta$ ,  $\gamma$ , l'une supérieure, l'autre inférieure à  $a_0$ .

On trouvera de même

$$P_3(\beta) = -\lambda_2 P_1(\beta),$$

$$P_3(\gamma) = -\lambda_2 P_1(\gamma),$$

mais  $P_1(\beta)$  est positif,  $P_1(\gamma)$  négatif; donc l'équation  $P_3(x) = 0$  a une racine supérieure à  $\beta$ , une autre comprise entre  $\beta$  et  $\gamma$ , enfin la troisième inférieure à  $\gamma$ .

En continuant ainsi, on voit que généralement les racines de  $P_{k-1}(x) = 0$  séparent les racines de  $P_k(x) = 0$ .

4. *Application des résultats précédents à la quadrature mécanique.* — Soit  $\mathcal{G}(x)$  un polynôme entier en  $x$ , du degré  $2n - 1$  au plus. La division de  $\mathcal{G}(x)$  par  $P_n(x)$  donnera

$$\mathcal{G}(x) = Q(x) P_n(x) + R(x);$$

le quotient  $Q(x)$ , ainsi que le reste  $R(x)$  étant tous les deux du degré  $\leq n - 1$  au plus.



faisant attention à (4), on en tire

$$\int_a^b f(x) \mathfrak{G}(x) dx = \int_a^b f(x) R(x) dx.$$

signons par  $x_1, x_2, \dots, x_n$  les racines de l'équation  $P_n(x) = 0$ ,  
es par ordre de grandeur croissante;  $R(x)$  étant du degré  $n - 1$ ,  
identiquement

$$R(x) = \frac{P_n(x)}{(x - x_1) P'_n(x_1)} R(x_1) + \dots + \frac{P_n(x)}{(x - x_n) P'_n(x_n)} R(x_n);$$

sant donc

$$\dots \dots A_k = \int_a^b f(x) \frac{P_n(x)}{(x - x_k) P'_n(x_k)} dx,$$

nt

$$\int_a^b f(x) \mathfrak{G}(x) dx = A_1 R(x_1) + \dots + A_n R(x_n),$$

$R(x_1) = \mathfrak{G}(x_1), \dots$ ; donc

$$\dots \int_a^b f(x) \mathfrak{G}(x) dx = A_1 \mathfrak{G}(x_1) + A_2 \mathfrak{G}(x_2) + \dots + A_n \mathfrak{G}(x_n),$$

constantes  $A_1, A_2, \dots, A_n$ , ne dépendent en aucune façon de la  
on  $\mathfrak{G}(x)$ .

*Propriétés des constantes  $A_k$ .* — La première de ces propriétés  
te en ce que tous les  $A_k$  sont positifs. Cela ne résulte pas immé-  
nent de la formule (9) qui a servi à leur définition, quoiqu'on  
ait le déduire de cette formule.

is il est plus facile de remarquer que la formule (10) subsiste  
un polynôme  $\mathfrak{G}(x)$  du degré  $2n - 1$  au plus, tout à fait arbitraire;

eurs, il est permis de prendre  $\mathfrak{G}(x) = \left[ \frac{P_n(x)}{x - x_k} \right]^2$ , ce qui donne

$$\dots \dots \int_a^b f(x) \left[ \frac{P_n(x)}{x - x_k} \right]^2 dx = A_k [P'_n(x_k)]^2,$$

résulte immédiatement la propriété énoncée.

Cette propriété est donc une conséquence nécessaire de (10), même dans le cas où l'équation (10) ne subsisterait qu'en prenant pour  $\mathfrak{S}(x)$  un polynôme du degré  $2n - 2$ .

Nous arrivons maintenant à une autre propriété plus cachée des  $A_k$ , que nous énonçons d'abord en écrivant les deux inégalités

$$(12) \quad A_1 + A_2 + A_3 + \dots + A_k > \int_a^{x_k} f(x) dx \quad (k = 1, 2, 3, \dots, n-1, n),$$

$$(13) \quad A_1 + A_2 + A_3 + \dots + A_k < \int_a^{x_{k+1}} f(x) dx \quad (k = 1, 2, 3, \dots, n-1).$$

La démonstration de ces inégalités dépend de nouveau de la formule (10), où nous prendrons pour  $\mathfrak{S}(x)$  un polynôme  $T(x)$  du degré  $n - 2$  défini par les conditions

$$\begin{aligned} T(x_1) &= 1, & T'(x_1) &= 0, \\ T(x_2) &= 1, & T'(x_2) &= 0, \\ &\dots & & \dots, \\ T(x_{k-1}) &= 1, & T'(x_{k-1}) &= 0, \\ T(x_k) &= 1, & & \\ T(x_{k+1}) &= 0, & T'(x_{k+1}) &= 0, \\ T(x_{k+2}) &= 0, & T'(x_{k+2}) &= 0, \\ &\dots & & \dots, \\ T(x_n) &= 0, & T'(x_n) &= 0. \end{aligned}$$

Le nombre de ces conditions étant  $2n - 1$ , et les quantités  $x_1, x_2, \dots, x_n$  étant inégales,  $T(x)$  est parfaitement défini, et l'on aura d'après (10),

$$(14) \quad \dots \int_a^b f(x) T(x) dx = A_1 + A_2 + A_3 + \dots + A_k.$$

Considérons maintenant l'équation

$$T'(x) = 0.$$

Nous voyons d'abord qu'elle admet les racines

$$\begin{aligned} x_1, x_2, x_3, \dots, x_{k-1}, \\ x_{k+1}, x_{k+2}, \dots, x_n \end{aligned}$$

un nombre de  $n - 1$ .

suite, le théorème de Rolle nous apprend l'existence de  $k-1$   
s

$$\xi_1, \xi_2, \xi_3, \dots, \xi_{k-1},$$

parent les quantités  $x_1, x_2, x_3, \dots, x_k$

in, le même théorème nous apprend l'existence des  $n-k-1$   
s

$$\eta_{k+2}, \eta_{k+3}, \dots, \eta_n$$

parent les quantités  $x_{k+1}, x_{k+2}, \dots, x_n$ .

nombre total des racines énumérées s'élève à  $2n-3$ , et, comme  
tion est du degré  $2n-3$ , elle n'en a pas d'autres. Nous voyons  
que toutes les racines de  $T'(x)=0$  sont réelles et inégales. Il s'en-  
que  $T'(x)$  change de signe chaque fois que  $x$  passe par une des ra-  
Les racines  $\xi_{k-1}$  et  $x_{k+1}$  sont deux racines consécutives, tandis  
est compris entre  $\xi_{k-1}$  et  $x_{k+1}$ . Mais  $T(x_k)=1$ ,  $T(x_{k+1})=0$ ;  
 $T'(x)$  est constamment négatif dans l'intervalle  $(\xi_{k-1}, x_{k+1})$ .

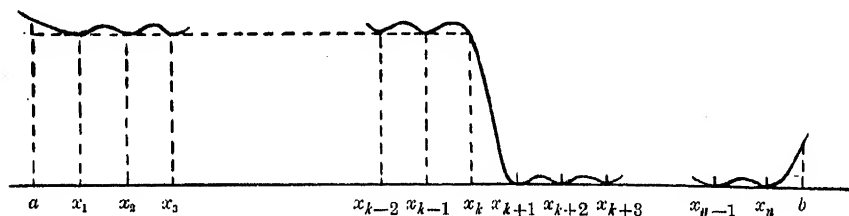
naissant maintenant le signe de  $T'(x)$ , dans un des intervalles  
is entre deux racines consécutives, on en déduit aussitôt le signe  
 $T(x)$  pour une valeur quelconque de  $x$ ; on trouve ainsi :

Intervalle.	Signe de $T'(x)$ .
$(a, x_1)$ . . . . .	—
$(x_1, \xi_1)$ . . . . .	+
$(\xi_1, x_2)$ . . . . .	—
$(x_2, \xi_2)$ . . . . .	+
. . . . .	..
$(x_{k-1}, \xi_{k-1})$ . . . . .	+
$(\xi_{k-1}, x_{k+1})$ . . . . .	—
$(x_{k+1}, \eta_{k+2})$ . . . . .	+
$(\eta_{k+2}, x_{k+2})$ . . . . .	—
. . . . .	..
$(x_{n-1}, \eta_n)$ . . . . .	+
$(\eta_n, x_n)$ . . . . .	—
$(x_n, b)$ . . . . .	+

près cela, on peut se représenter facilement la série des valeurs  
rend le polynôme  $T(x)$ , et qui est indiquée dans la figure ci-

On voit :

- 1<sup>o</sup> Que  $T(x)$  ne devient pas négatif dans l'intervalle  $(a, b)$ ;
- 2<sup>o</sup> Que  $T(x)$  ne devient pas inférieur à l'unité dans l'intervalle  $(a, x_k)$ .



Dès lors nous pouvons conclure de l'équation (14)

$$A_1 + A_2 + \dots + A_k \geq \int_a^{x_k} f(x) T(x) dx.$$

Le signe  $=$  ne saurait convenir que lorsque l'intervalle  $(A, B)$  dont nous supposons l'existence (n<sup>o</sup> 1) tombe entièrement dans l'intervalle  $(a, x_k)$ . En remplaçant enfin  $T(x)$  par sa valeur minima dans l'intervalle  $(a, x_k)$ , qui est égale à l'unité, nous avons, dans tous les cas,

$$A_1 + A_2 + \dots + A_k > \int_a^{x_k} f(x) dx.$$

Ce raisonnement s'applique aux valeurs 1, 2, 3, ...,  $n-1$  de  $k$ ; après une remarque que l'on trouvera plus loin (n<sup>o</sup> 7), cette inégalité reste encore vraie pour  $k=n$ .

Quant à l'inégalité (13), on pourrait la déduire d'une manière analogue; mais il est un peu plus court de remarquer qu'on démontrera précisément de la même manière que (12), cette autre inégalité

$$A_{k+1} + A_{k+2} + \dots + A_n > \int_{x_{k+1}}^b f(x) dx \quad (k=1, 2, 3, \dots, n-1),$$

en considérant l'autre limite  $(b)$  de l'intégrale. Or

$$A_1 + A_2 + \dots + A_n = \int_a^b f(x) dx;$$

, par soustraction,

$$A_1 + A_2 + \dots + A_k < \int_a^{x_k+1} f(x) dx.$$

nous savons déjà que  $A_k$  est positif; cela se confirme de nouveau par les inégalités (12), (13) en remplaçant dans la dernière  $k$  par  $k-1$ .

Avant d'aller plus loin dans les considérations générales, nous allons maintenant considérer un cas spécial, celui de la quadrature de Gauss, où  $f(x) = 1$ .

*Sur la quadrature de Gauss.* — Supposons donc  $f(x) = 1$ , et pour simplifier (sans nuire réellement à la généralité),  $a = -1$ ,  $b = +1$ . Alors, comme l'on sait, le polynôme  $P_n(x)$  ne se distingue que par un facteur constant du polynôme  $X_n$  de Legendre. Les inégalités (12) et (13) deviennent

$$\left. \begin{aligned} & \dots \dots \dots \left\{ \begin{aligned} & -1 + A_1 + A_2 + \dots + A_k > x_k, \\ & -1 + A_1 + A_2 + \dots + A_k < x_{k+1}. \end{aligned} \right. \end{aligned}$$

Supposons maintenant qu'on applique la quadrature à une fonction  $\mathfrak{F}(x)$  quelconque; on aura pour valeur approchée de

$$\int_{-1}^{+1} \mathfrak{F}(x) dx$$

l'expression

$$\dots \dots \dots A_1 \mathfrak{F}(x_1) + A_2 \mathfrak{F}(x_2) + \dots + A_n \mathfrak{F}(x_n).$$

Mais, d'après les inégalités (14),  $x_1, x_2, x_3, \dots$  tombent dans les intervalles

$$\begin{aligned} & (-1, -1 + A_1), (-1 + A_1, -1 + A_1 + A_2), \\ & (-1 + A_1 + A_2, -1 + A_1 + A_2 + A_3), \dots \end{aligned}$$

Cette expression (15) rentre donc dans celle-ci, qui sert de définition de l'intégrale  $\int_{-1}^{+1} \mathfrak{F}(x) dx$ ,

$$\lim [\delta_1 \mathfrak{F}(\xi_1) + \delta_2 \mathfrak{F}(\xi_2) + \dots + \delta_n \mathfrak{F}(\xi_n)],$$

comme les différences  $x_1 + 1, x_2 - x_1, x_3 - x_2, \dots$  deviennent

infinitement petites avec  $\frac{1}{n}$ , nous arrivons à cette conclusion, que l'expression (15) donnera avec une approximation indéfinie la valeur de  $\int_{-1}^{+1} \mathfrak{F}(x) dx$ , en augmentant  $n$ , toutes les fois que  $\mathfrak{F}(x)$  est intégrable dans l'intervalle  $(-1, +1)$ , et reste comprise entre deux limites finies.

7. *Sur la distribution des racines de l'équation  $P_n(x) = 0$ .* — Dans le cas spécial que nous venons de considérer, les connaissances acquises sur les polynômes de Legendre nous ont permis de conclure que les racines  $x_1, x_2, \dots, x_n$  sont distribuées de manière que les quantités  $+1, x_2 - x_1, \dots, x_n - x_{n-1}, 1 - x_n$  deviennent infinitement petites avec  $\frac{1}{n}$ . Il nous reste à chercher la proposition analogue pour le cas général. Voici une première observation à cet égard :

Supposons d'abord qu'il existe un nombre  $a_1$  plus grand que  $a$ , mais plus petit que  $b$ , tel que

$$\int_a^{a_1} f(x) dx = 0,$$

encore aussi

$$\int_a^{a_1} x^k f(x) dx = 0.$$

Il est évident alors que le polynôme  $P_n(x)$ , que nous déterminons, sera identique à celui qu'on aurait obtenue en considérant directement les limites  $a_1$  et  $b$  au lieu de  $a$  et  $b$ . Les racines de  $P_n(x) = 0$  seront donc comprises dans l'intervalle  $(a_1, b)$  (excluant les limites), et il n'y aura aucune racine dans l'intervalle  $(a, a_1)$ . Une remarque analogue s'applique à l'autre limite  $b$ , et nous pouvons donc dire que, lorsqu'un intervalle  $(a, \beta)$ , tel que

$$\int_a^\beta f(x) dx = 0,$$

tend jusqu'à une des limites  $a$  ou  $b$ , cet intervalle ne comprendra aucune racine de  $P_n(x) = 0$ .

Mais nous ajoutons maintenant que, lorsque cet intervalle  $(a, \beta)$  ne tend pas jusqu'à une des limites  $a$  ou  $b$ , cet intervalle (incluant les limites  $a, \beta$ ) ne comprend jamais plus d'une racine.

st, en effet, une conséquence immédiate des inégalités (12) et (13),  
onnent

$$\int_{x_k}^{x_{k+1}} f(x) dx > 0 \quad (k = 1, 2, 3, \dots, n-1).$$

es exemples font voir, du reste, que les deux cas, où un tel inter-  
( $\alpha, \beta$ ) comprend une ou aucune racine, se présentent tous les

posons, par exemple, que la fonction  $f(x)$  ait la propriété  
née par l'équation

$$f(a+x) = f(b-x);$$

on verra facilement que, à chaque racine  $x_1$  de  $P_n(x) = 0$ , corres-  
une racine  $a+b-x_1$ . Supposons de plus que  $f(x)$  soit con-  
nent égale à zéro dans l'intervalle  $(\frac{a+b}{2} - h, \frac{a+b}{2} + h)$ ; alors,  
t pair, il n'y aura aucune racine de  $P_n(x)$  dans cet intervalle (parce  
ne peut y en avoir deux); mais si  $n$  est impair, la racine  $\frac{a+b}{2}$   
dans cet intervalle, et c'est la seule.

us allons maintenant démontrer la proposition suivante:

( $\alpha, \beta$ ) un intervalle quelconque, faisant partie de l'intervalle  
étendu ( $a, b$ ) et tel que

$$\int_{\alpha}^{\beta} f(x) dx$$

e valeur positive différente de zéro; alors, pour toutes les valeurs  
dessus d'une certaine limite, au moins une racine de  $P_n(x) = 0$   
e dans cet intervalle ( $\alpha, \beta$ ).

nons un intervalle ( $\alpha', \beta'$ ),  $\alpha < \alpha' < \beta' < \beta$ , tel que

$$\int_{\alpha'}^{\beta'} f(x) dx = M,$$

nt une valeur positive, ce qui est possible, d'après la supposition  
ous avons faite.

Construisons maintenant un polynôme  $T(x)$  d'un degré fini  $k$ , tel

$$\begin{aligned} \text{Val. abs. } T(x) < \varepsilon, \quad a \leq x \leq a, \quad \beta \leq x \leq b, \\ T(x) \geq 1, \quad a' \leq x \leq \beta', \end{aligned}$$

supposons de plus que  $T(x)$  soit positif dans l'intervalle  $(a, a')$  et dans l'intervalle  $(\beta', \beta)$ . Admettons pour un moment l'existence d'un polynôme  $T(x)$  d'un degré fini  $k$ ,  $\varepsilon$  étant une quantité arbitraire. Or, lorsque  $n$  est supérieur à  $\frac{1}{2}k$ , il y aura au moins une racine de  $T(x)$  dans l'intervalle  $(a, \beta)$ .

En effet, supposons que cela n'eût pas lieu. Parce que  $n > \frac{1}{2}k$ , on exactement

$$\int_a^b f(x) T(x) dx = A_1 T(x_1) + \dots + A_n T(x_n),$$

cette intégrale serait inférieure à

$$\varepsilon (A_1 + A_2 + \dots + A_n) = \varepsilon \int_a^b f(x) dx.$$

Mais, d'autre part, il est évident que la valeur de cette intégrale supérieure à

$$M - \varepsilon \int_a^b f(x) dx,$$

qui implique contradiction,  $\varepsilon$  étant arbitraire.

Quant à l'existence du polynôme  $T(x)$ , on peut s'en convaincre si qu'il suit:

Soit  $F(x)$  une fonction continue, à un nombre fini de maxima et minima, dans l'intervalle  $(a, b)$ . En posant

$$\frac{b + a - 2x}{b - a} = \cos \varphi,$$

aura

$$F(x) = \mathfrak{G}(\varphi)$$

les limites  $x = a$ ,  $x = b$  correspondent à  $\varphi = 0$ ,  $\varphi = \pi$ ;  $\mathfrak{G}(\varphi)$  est développable en une série telle que

$$\frac{1}{2} a_0 + a_1 \cos \varphi + a_2 \cos 2 \varphi + \dots,$$



cette série converge uniformément, c'est-à-dire qu'on peut prendre  $\varepsilon$  assez grand pour que

$$\mathfrak{G}_1(\varphi) = \frac{1}{2} a_0 + a_1 \cos \varphi + \dots + a_k \cos k \varphi$$

et, pour toutes les valeurs, de  $\varphi = 0$  jusqu'à  $\varphi = \pi$ , moins que  $\varepsilon$  ( $\varphi$ ). En introduisant  $x$  au lieu de  $\varphi$ , on aura ainsi un polynôme  $F_1(x)$  de degré  $k$ , tel que

$$\text{val. abs. } [F(x) - F_1(x)] < \varepsilon \quad (a \leq x \leq b).$$

A l'aide de ce résultat, il est facile de voir qu'il existe, en effet, un polynôme  $T(x)$ , doué des propriétés que nous avons supposées. En résumant les résultats obtenus, nous pouvons conclure que, augmentant indéfiniment, les intégrales

$$f(x) dx, \int_{x_1}^{x_2} f(x) dx, \int_{x_2}^{x_3} f(x) dx, \dots, \int_{x_{n-1}}^{x_n} f(x) dx, \int_{x_n}^b f(x) dx$$

convergent toutes vers zéro, sans qu'on puisse dire la même chose des différences

$$x_1 - a, x_2 - x_1, x_3 - x_2, \dots, x_n - x_{n-1}, b - x_n.$$

Après les inégalités (12), (13), on a

$$A_1 + A_2 + \dots + A_k < \int_a^{x_{k+1}} f(x) dx,$$

$$A_1 + A_2 + \dots + A_{k-1} > \int_a^{x_k} f(x) dx;$$

$$A_k < \int_{x_{k-1}}^{x_{k+1}} f(x) dx,$$

ce qui fait voir, d'après ce qui précède, que les  $A_k$  convergent vers zéro avec  $\frac{1}{n}$ .

*Application des résultats obtenus.* — On ne saurait douter, il semble, que les propositions que nous avons obtenues seront

un grand usage, si l'on veut étudier la question que nous avons  
sée au début de l'introduction.

Toutefois, en considérant l'intégrale

$$\int_a^b f(x) F(x) dx,$$

conditions à imposer aux fonctions  $f(x)$ ,  $F(x)$  deviennent la source  
difficultés qu'on ne saurait vaincre qu'à l'aide de nouvelles re-  
cherches sur les principes mêmes du Calcul intégral.

Je me contenterai seulement de considérer un cas assez simple.  
soujettissons la fonction  $f(x)$  à cette nouvelle condition, qu'il n'existe  
s un intervalle  $(\alpha, \beta)$  tel que

$$\int_{\alpha}^{\beta} f(x) dx = 0.$$

En posant

$$y = \int_a^x f(x) dx,$$

sera donc une fonction continue de  $x$ , toujours croissante, et, en  
sant

$$x = \psi(y),$$

fonction  $\psi(y)$  sera de même continue et toujours croissante.

En introduisant  $y$  au lieu de  $x$ , il vient

$$\int_a^b f(x) F(x) dx = \int_0^c F[\psi(y)] dy, \quad c = \int_a^b f(x) dx.$$

Déterminons maintenant les constantes  $\xi_1, \xi_2, \dots, \xi_{n-1}$  par

$$A_1 + A_2 + \dots + A_k = \int_a^{\xi_k} f(x) dx;$$

aura, d'après (12) et (13),

$$x_k < \xi_k < x_{k+1}.$$

Désignons encore par  $y_k, \eta_k$  les valeurs de  $y$  correspondant aux

ours  $x_k$ ,  $\xi_k$  de  $x$ , l'expression

$$A_1 F(x_1) + A_2 F(x_2) + \dots + A_n F(x_n)$$

endra

$$\eta_1 F[\psi(y_1)] + (\eta_2 - \eta_1) F[\psi(y_2)] + \dots + (c_n - \eta_{n-1}) F[\psi(y_n)];$$

comme on a

$$0 < y_1 < \eta_1 < y_2 < \eta_2 < \dots < \eta_{n-1} < y_n < c,$$

expression rentre dans celle qui sert de définition à  $\int_0^c F[\psi(y)] dy$ .

plus, d'après les recherches du n° 7, les intervalles deviennent  
 ment petits avec  $\frac{1}{n}$ .

nsi encore, dans ce cas, la quadrature peut donner une approxi-  
 on indéfinie, à la seule condition que  $F(x)$  soit intégrable.

---

## XXXII.

(Paris, C.-R. Acad. Sci., 99, 1884, 508—509.)

### Sur un développement en fraction continue.

(Note, présentée par M. Tisserand.)

Supposons que  $A_1 F(x_1) + A_2 F(x_2) + \dots + A_n F(x_n)$  soit l'expression approchée de l'intégrale  $\int_{-1}^{+1} F(x) dx$  donnée par la quadrature de Gauss.

Dans un Mémoire inséré dans les Annales de l'Ecole Normale 34, p. 420) j'ai démontré les inégalités suivantes

$$\left. \begin{aligned} & -1 < x_1 < -1 + A_1 < x_2 < -1 + A_1 + A_2 < x_3 < \dots \\ & < -1 + A_1 + \dots + A_{n-1} < x_n < +1. \end{aligned} \right\}$$

Considérons maintenant la fraction continue

$$\Omega = \frac{2}{1 \cdot 1} \\ z - \frac{1 \cdot 3}{3 \cdot 3} \\ z - \frac{5 \cdot 7}{4 \cdot 4} \\ z - \frac{7 \cdot 9}{z - \dots}$$

soit  $\frac{P_n}{Q_n}$  la réduite d'ordre  $n$ . On sait que  $x_1, x_2, \dots, x_n$  sont les racines de l'équation  $Q_n = 0$ , et la décomposition en fractions simples en est

$$\frac{P_n}{Q_n} = \frac{A_1}{z - x_1} + \frac{A_2}{z - x_2} + \dots + \frac{A_n}{z - x_n}.$$

Supposons que  $z$  ait une valeur quelconque réelle ou imaginaire, mais non comprise dans l'intervalle réel  $(-1, +1)$ . Alors, en vertu

inégalités (1) et de la définition même d'une intégrale définie, le second membre de (2) converge, lorsque  $n$  augmente indéfiniment vers une limite déterminée qui n'est autre chose que l'intégrale (il s'agit de)  $\int_{-1}^{+1} \frac{dx}{z-x}$  : donc

$$\lim \frac{P_n}{Q_n} = \int_{-1}^{+1} \frac{dx}{z-x}.$$

Par conséquent, la fraction continue  $\Omega$  converge dans tout le plan, exceptant la coupure rectiligne de  $-1$  à  $+1$ .

On voit encore facilement que la fraction continue converge uniformément dans le voisinage de toute valeur particulière appartenant à la région de convergence.

Ce résultat est connu, mais la démonstration précédente semble simple; de plus, elle est applicable encore à la fraction con-

vergente que l'on obtient pour l'intégrale  $\int_a^b \frac{f(x)}{z-x} dx$ ,  $f(x)$  étant une fonction qui ne devient pas négative dans l'intervalle  $(a, b)$ .

# XXXIII.

(Bull. astr., Paris, 1, 1884, 465—467.)

---

## Note sur la densité de la Terre.

Nous considérons la Terre comme composée de couches ellipsoïdales homogènes de révolution. Soient

$x$  le demi-petit axe,

$\varrho_x$  la densité d'une couche quelconque.

Nous prendrons pour unité de longueur la valeur de  $x$  à la surface et nous désignerons par  $\Delta$  la densité moyenne de la Terre, enfin par  $\lambda$  la fraction

$$\frac{\int_0^1 x^2 \varrho_x dx}{\int_0^1 x^4 \varrho_x dx}.$$

Supposons connues les valeurs de  $\Delta$  et de  $\lambda$ , ainsi que la valeur  $\varrho_1$  de la densité à la surface.

Dans ces conditions, il est possible de déterminer une limite inférieure de la densité  $\varrho_0$  au centre, en admettant que  $\varrho_x$  ne croît jamais avec  $x$ .

Posons  $A = \int_0^1 x^2 \varrho_x dx$ ,  $B = \int_0^1 x^4 \varrho_x dx$ , en sorte qu'on a

$$A = \frac{1}{3} \Delta, \quad B = \frac{\Delta}{3\lambda}.$$

Une intégration par parties donne

$$\dots \dots \dots 3 A - \varrho_1 = - \int_0^1 x^3 \varrho'_x dx,$$

$$\dots \dots \dots 5 B - \varrho_1 = - \int_0^1 x^5 \varrho'_x dx,$$

dis qu'on a évidemment

$$\dots \dots \dots \varrho_0 - \varrho_1 = - \int_0^1 \varrho'_x dx.$$

on déduit aussitôt

$$(\varrho_0 - \varrho_1)^3 (\varrho_0 - \varrho_1)^2 - (3 A - \varrho_1)^5$$

$$= - \int_0^1 \int_0^1 \int_0^1 \int_0^1 \int_0^1 (x^5 y^5 z^5 t^5 u^5) \varrho'_x \varrho'_y \varrho'_z \varrho'_t \varrho'_u dx dy dz dt du.$$

La notation des variables étant arbitraire, on peut dans le second membre permuter de toutes les manières possibles les lettres  $x, y, z, t, u$ . On obtient ainsi en tout dix expressions du premier membre, et prenant la moyenne,

$$\dots \dots \dots \left\{ \begin{aligned} & (5 B - \varrho_1)^3 (\varrho_0 - \varrho_1)^2 - (3 A - \varrho_1)^5 \\ & = - \int_0^1 \int_0^1 \int_0^1 \int_0^1 \int_0^1 T \varrho'_x \varrho'_y \varrho'_z \varrho'_t \varrho'_u dx dy dz dt du, \end{aligned} \right. \dots$$

$$T = \frac{1}{120} (\Sigma x^5 y^5 z^5) - x^3 y^3 z^3 t^3 u^3.$$

si  $a_1, a_2, a_3, \dots, a_n$  sont des nombres positifs, on voit facilement que la valeur moyenne de tous les produits de ces nombres trois à trois est supérieure à la troisième puissance de leur moyenne géométrique  $\sqrt[n]{a_1 a_2 \dots a_n}$ . En appliquant cette remarque aux cinq nombres  $x^5, y^5, z^5, t^5, u^5$ , on voit que  $T$  est toujours positif ou du moins jamais négatif. En y regardant de plus près, on trouve que  $T$  est égal à zéro seulement dans les cas suivants :

1°.  $x = y = z = t = u$ ;

2°. Quand au moins trois des nombres  $x, y, z, t, u$  s'évanouissent.

Mais, par hypothèse, la dérivée  $\varrho'_x$  n'est jamais positive: donc

$$(5 B - \varrho_1)^3 (\varrho_0 - \varrho_1)^2 - (3 A - \varrho_1)^5 \geq 0$$

bien

$$\varrho_0 \geq \varrho_1 + \sqrt{\frac{(3A - \varrho_1)^5}{(5B - \varrho_1)^3}},$$

t-à-dire

$$\dots \varrho_0 \geq \varrho_1 + \sqrt{\frac{(\Delta - \varrho_1)^5}{\left(\frac{5\Delta}{3\lambda} - \varrho_1\right)^3}} = \varrho_1 + (\Delta - \varrho_1) \sqrt{\frac{(\Delta - \varrho_1)^8}{\left(\frac{5\Delta}{3\lambda} - \varrho_1\right)^8}}.$$

En adoptant pour  $\Delta$  la valeur 5,56 d'après MM. Cornu et Baillet-Latour (Comptes rendus, t. LXXXVI) et  $\varrho_1 = 2,6$ ,  $\lambda = 1,9553$ , la dernière valeur étant empruntée à M. Tisserand (Bull. astr., t. I., p. 419), on obtient  $\varrho_0 \geq 7,418$ .

Il convient de remarquer que la limite inférieure que nous venons d'obtenir ne saurait être remplacée par une autre plus élevée, parce qu'elle correspond à la distribution suivante de la masse de la Terre:

$$\varrho_x = \varrho_0, \text{ de } x = 0 \text{ jusqu'à une certaine valeur } x = a < 1,$$

$$\varrho_x = \varrho_1, \text{ de } x = a \text{ jusqu'à } x = 1.$$

On trouve alors

$$3A = \varrho_0 x^3 + \varrho_1 (1 - x^3),$$

$$5B = \varrho_0 x^5 + \varrho_1 (1 - x^5)$$

bien

$$3A - \varrho_1 = x^3 (\varrho_0 - \varrho_1),$$

$$5B - \varrho_1 = x^5 (\varrho_0 - \varrho_1).$$

Ces deux équations déterminent les inconnues  $\varrho_0$  et  $x$ , et il est facile de voir que la valeur de  $\varrho_0$  qu'on en déduit coïncide avec la limite inférieure que nous venons d'obtenir.

La valeur de  $x$

$$x = \sqrt{\frac{5B - \varrho_1}{3A - \varrho_1}} = \sqrt{\frac{\frac{5\Delta}{3\lambda} - \varrho_1}{\Delta - \varrho_1}}$$

pour être inférieure à l'unité, on doit avoir  $\lambda > \frac{5}{3}$ , ce qu'on voit facilement par l'inspection des formules (1) et (2).



## XXXIV.

Amsterdam, Versl. K. Akad. Wet. sér. 3, 1, 1885, 272—297).

Reimprimé: Haarlem, Arch. Néerl. Sci. Soc. Holl., 19,

1884, 435—460.)

### Quelques remarques sur la variation de la densité dans l'intérieur de la Terre.

#### INTRODUCTION.

Considérons la terre comme formée de couches ellipsoïdales, que la densité  $f$  soit constante dans l'étendue de chacune d'elles et que le rayon de ces couches sera déterminée par le rayon  $x$  de la sphère équivalente et nous supposons qu'à la surface on ait  $x=1$ .

Soit de ces notations que le volume de la terre est  $\frac{4}{3}\pi$ , sa masse

$M = \int_0^1 x^2 f(x) dx$ . Donc la densité moyenne  $\Delta = 3 \int_0^1 x^2 f(x) dx$ .

Or, ce qui suit, je suppose connu  $\Delta$ , ainsi que le rapport

$$\lambda = \frac{\int_0^1 x^2 f(x) dx}{\int_0^1 x^4 f(x) dx},$$

on peut obtenir la valeur en combinant les observations astronomiques avec celles qui servent à faire connaître la figure de la

terre, comme dernière donnée, je prendrai la valeur de la densité à la surface:  $f(1) = d$ .

Sous ces conditions mon but est de limiter, autant que possible, la recherche de la fonction inconnue  $f(x)$ . Cela n'est possible qu'à l'aide de certaines hypothèses: les deux suivantes seront discutées successivement.

I. La densité va continuellement en croissant de la surface jusqu'au centre de la terre.

II. La densité va continuellement en croissant de la surface jusqu'au centre, mais la rapidité de cet accroissement va en diminuant la surface jusqu'au centre.

Enfin, dans une troisième partie, je considérerai brièvement la mise en nombres des résultats obtenus, et j'ajouterai une discussion de différentes formules qu'on a proposées pour représenter la densité dans l'intérieur de la terre.

Mais, avant d'entrer en matière, voici quelques remarques préliminaires qui se rapportent également à la discussion des deux hypothèses.

D'abord il convient d'introduire au lieu de  $\Delta$  et  $\lambda$  les intégrales

$$\dots\dots\dots A = \int_0^1 x^2 f(x) dx,$$

$$\dots\dots\dots B = \int_0^1 x^4 f(x) dx,$$

$$\text{sorte qu'on a } A = \frac{\Delta}{3}, B = \frac{\Delta}{3\lambda}.$$

Ensuite, démontrons la proposition suivante:

„Lorsque deux fonctions  $F(x)$ ,  $G(x)$  vérifient les équations

$$\dots\dots\dots \int_0^1 x^2 F(x) dx = A, \int_0^1 x^4 F(x) dx = B,$$

$$\dots\dots\dots \int_0^1 x^2 G(x) dx = A, \int_0^1 x^4 G(x) dx = B,$$

alors la différence  $F(x) - G(x)$ , si elle n'est pas constamment égale à zéro, doit changer au moins deux fois de signe dans l'intervalle de zéro à l'unité”.

En effet les équations (3) et (4) donnent

$$\dots\dots\dots \int_0^1 x^2 [F(x) - G(x)] dx = 0,$$

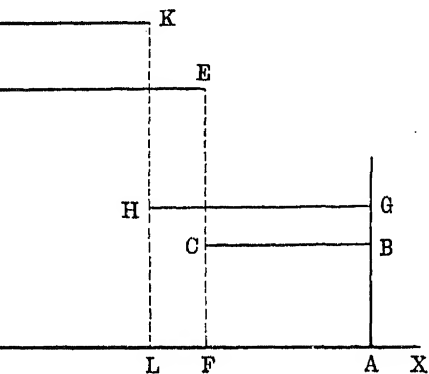
$$\dots\dots\dots \int_0^1 x^4 [F(x) - G(x)] dx = 0,$$

d'où il est évident que  $F(x) - G(x)$  doit changer de signe au moins deux fois.

ne on le voit par les inégalités (7), la valeur de  $a$  est inférieure à 1; quant à  $m = d + \frac{3A-d}{a^3}$ , à cause de  $a < 1$  il vient  $m > 3A$ , c'est-à-dire  $m$  est supérieur à la densité moyenne de la terre, ce qui est évident a priori.

En prenant (Fig. 1) un système d'axes rectangulaires  $O X, O Y, O Z$ ,  $O F = a$ ,  $O D = m$ ,  $A B = d$ , cette loi de densité est représentée par les deux droites  $D E, C B$ . Or il est évident maintenant que  $m$  est la densité minima au centre, c'est-à-dire qu'il n'y a aucune loi de densité qui donne pour  $x = 0$  une densité inférieure à  $m$ . En effet, désignons par  $f(x)$  la loi de densité représentée par  $D E, C B$ , et par  $f_1(x)$  une autre loi de densité, qui donnerait au centre une densité

Fig. 1.



inférieure à  $m$ ; on voit aussitôt que  $f(x) - f_1(x)$  ne pourrait présenter qu'un seul changement de signe, ce qui est impossible d'après la proposition du n° 1.

Dans la suite, la limite inférieure de la densité pour  $x = b$  est désignée par  $t(b)$  et la limite supérieure de cette même densité par  $T(b)$ . Le résultat que nous venons d'obtenir s'exprime donc par  $t(0) = m$ , tandis qu'on a évidemment  $t(1) = d$ ,  $T(1) = d$ .

Nous nous proposons de déterminer ces fonctions  $t(b)$ ,  $T(b)$  pour une valeur quelconque de  $b$ .

En premier lieu, il est évident, en jetant un regard sur la Fig. 1, que

$$t(b) = d, \quad a \leq b \leq 1,$$

avec l'aide d'un raisonnement, tout-à-fait analogue à celui qui nous a permis de voir que  $t(0) = m$ , on se convainc que

$$T(a) = m.$$

LA DENSITÉ DANS L'INTÉRIEUR DE LA TERRE. 403

La fonction  $t(b)$  étant connue maintenant pour les valeurs de  $b$  comprises entre  $a$  et l'unité, il reste seulement à trouver la valeur de  $t(b)$  pour les valeurs positives de  $b$  inférieures à  $a$ . (Nous savons déjà que  $t(0) = m$ ).

Pour cela, je cherche une fonction  $F(x)$ , ainsi

$$F(x) = K, \quad 0 < x < b,$$

$$F(x) = k, \quad b < x < 1,$$

et  $k$  étant des constantes qui doivent être déterminées par les conditions (3). Un calcul facile donne

$$K = \frac{3(1 - b^5)A - 5(1 - b^3)B}{b^3(1 - b^2)},$$

$$k = \frac{5B - 3b^2A}{1 - b^2}.$$

La valeur de  $k$ , considérée comme fonction de  $b$ , est décroissante, et comme on voit facilement que pour  $b = a$  il vient  $k = d$ , la valeur de  $k$  sera supérieure à  $d$  dans l'hypothèse actuelle  $0 < b < a$ . D'après la proposition du n° 1 on en conclut  $K > m$ . Dans la Fig. 1 la fonction  $F(x)$  est représentée par les droites IK et HG, et  $b$  par OL.

On voit maintenant, d'après un raisonnement déjà développé plus d'une fois, qu'il ne peut exister une loi de densité qui donne pour  $x = b$  une densité inférieure à  $k$  ou supérieure à  $K$ ; donc  $t(b) \geq k$ ,  $T(b) \leq K$ .

La fonction  $F(x)$  n'est pas, à proprement parler, une fonction qui puisse être assimilée à la densité, parce qu'on a  $T(1) = k > d$ . Mais on peut se figurer une loi de densité qui diffère très peu de  $F(x)$  dans tout l'intervalle de zéro à l'unité et qui présente seulement dans le voisinage de la surface un changement extrêmement rapide de  $k$  à  $d$ .

D'après cette remarque, on doit avoir:  $t(b) = k$ ,  $T(b) = K$ , c à d.

$$t(b) = \frac{5B - 3b^2A}{1 - b^2}, \quad T(b) = \frac{3(1 - b^5)A - 5(1 - b^3)B}{b^3(1 - b^2)}$$

sous la condition  $0 < b \leq a$ .

La fonction  $t(b)$  est maintenant parfaitement connue. Remarquons

se présente une discontinuité; en effet,  $\varepsilon$  étant infiniment petit,

$$t(\varepsilon) = 5B < 3A$$

$$t(0) = m > 3A.$$

La singularité s'explique très bien si l'on fait attention à la différence qui existe entre les deux lois de densité qui donnent la densité minima au centre et la densité minima dans un point du centre.

Il reste à déterminer  $T(b)$  pour les valeurs de  $b$  comprises entre  $a$  et 1. J'observe pour cela que

$$B = \int_0^b x^4 f(x) dx + \int_b^1 x^4 f(x) dx,$$

$$B \geq f(b) \int_0^b x^4 dx + f(1) \int_b^1 x^4 dx,$$

$$B \geq \frac{1}{5} b^5 f(b) + \frac{1-b^5}{5} d,$$

il en résulte

$$f(b) \leq \frac{5B - (1-b^5)d}{b^5}.$$

Il est évident par là qu'on doit avoir aussi

$$T(b) \leq \frac{5B - (1-b^5)d}{b^5}.$$

En fait, une simple limitation de  $T(b)$ , qu'on pourrait facilement obtenir dans l'intervalle  $0 < b \leq a$  où nous connaissons déjà la valeur de  $T(b)$ . On voit aussi que pour  $b=a$  il faut mettre le signe = dans la relation (10).

Je dis maintenant qu'on a pour toute valeur de  $b$  comprise entre  $a$  et 1

$$T(b) = \frac{5B - (1-b^5)d}{b^5}.$$

Pour le démontrer en toute rigueur, il faudrait faire voir que,

estant une quantité inférieure à  $\frac{5B - (1 - b^5)d}{b^5}$  mais en différant si peu qu'on le veut, il existe toujours une loi de densité telle que  $f(b) = R$ . Mais il me semble que l'indication suivante suffit.

Soit

$$\begin{aligned}\varphi(x) &= \frac{5B - (1 - b^5)d}{b}, & 0 \leq x \leq b, \\ \varphi(x) &= d, & b \leq x \leq 1,\end{aligned}$$

on vérifie sans peine que

$$\int_0^1 x^4 \varphi(x) dx = B.$$

Si l'on désignait par  $A'$  la valeur de l'intégrale  $\int_0^1 x^2 \varphi(x) dx$ , on trouve

$$A' = \frac{5B - d + b^2 d}{3b^2}.$$

Considérée comme fonction de  $b$ ,  $A'$  est décroissante, et pour  $b = a$ ,  $A' = A$ ; donc, dans la supposition  $a < b < 1$ ,  $A'$  est inférieure à  $A$ .

La fonction  $\varphi(x)$  ne satisfait donc pas aux conditions imposées à la densité, mais en posant

$$\begin{aligned}f(x) &= \varphi(x), & \varepsilon < x < 1, \\ f(x) &= \varphi(x) + \frac{A - A'}{\varepsilon x^2}, & 0 < x < \varepsilon,\end{aligned}$$

où  $\varepsilon$  est une quantité aussi petite qu'on voudra, il vient

$$\int_0^1 x^2 f(x) dx = A' + \int_0^\varepsilon \frac{A - A'}{\varepsilon} dx = A,$$

$$\int_0^1 x^4 f(x) dx = B + \int_0^\varepsilon \frac{A - A'}{\varepsilon} x^2 dx = B + \frac{1}{3} (A - A') \varepsilon^2.$$

En prenant  $\varepsilon$  infiniment petit, la fonction  $f(x)$  satisfait donc bien aux conditions imposées à la densité et l'on a  $f(b) = \frac{5B - (1 - b^5)d}{b^5}$ .

D'une manière sommaire, mais peu exacte, on pourrait dire que, pour avoir la plus grande densité pour  $x = b > a$ , il faut se figurer

me condensée dans le centre de la terre une partie finie de la  
 se totale de la terre. Cette partie de la masse a alors une in-  
 ce appréciable dans l'intégrale  $\int_0^1 x^2 f(x) dx$ , mais elle ne change  
 rien la valeur de  $\int_0^1 x^4 f(x) dx$ , à cause du facteur  $x^4$ .  
 n réunissant les résultats obtenus, on a les formules suivantes

$$\begin{aligned} & \left\{ \begin{aligned} t(0) &= m, \\ t(b) &= \frac{5B - 3b^2 A}{1 - b^3}, & 0 < b \leq a, \\ t(b) &= d, & a \leq b \leq 1, \end{aligned} \right. \\ & \left\{ \begin{aligned} T(b) &= \frac{3(1 - b^5) A - 5(1 - b^3) B}{b^3(1 - b^3)}, & 0 < b \leq a, \\ T(b) &= \frac{5B - (1 - b^5) d}{b^5}, & a \leq b < 1. \\ T(1) &= d. \end{aligned} \right. \end{aligned}$$

La fonction  $T(b)$  présente une discontinuité; en effet,  $\varepsilon$  étant in-  
 finiment petit, on a

$$\begin{aligned} T(1 - \varepsilon) &= 5B > d, \\ T(1) &= d. \end{aligned}$$

## DEUXIÈME PARTIE.

### Discussion de l'hypothèse II.

Dans ce qui suit, nous admettrons: -

- que la fonction  $f(x)$  ne croît jamais avec  $x$ ,
- que la fonction  $\frac{df(x)}{dx}$  ne croît jamais avec  $x$ .

Quant à cette seconde condition, elle semble exiger l'existence  
 de la fonction dérivée  $\frac{df(x)}{dx}$ ; pour cette raison, il vaut mieux  
 énoncer un peu autrement, en disant que, sous la condition

$$0 \leq x < y < z \leq 1,$$

il doit avoir toujours

$$\frac{f(x) - f(y)}{y - x} \leq \frac{f(y) - f(z)}{z - y}.$$

avons une différence profonde qui existe entre notre hypothèse  
elle et celle que nous venons de discuter. Dans la première hy-  
pothèse, la fonction  $f(x)$  peut avoir un saut brusque pour une valeur  
quelconque de  $x$ ; on voit facilement que cela n'est plus possible  
maintenant, à cause de la condition (13), que pour la seule valeur

On va d'abord quelles relations l'hypothèse actuelle entraîne entre  
les données  $A, B, d$ .

Naturellement, on a comme auparavant,  $3A > 5B > d$ , mais il existe  
une autre relation, propre à notre hypothèse. Pour la trouver,  
définissons la fonction  $F(x)$ , qui s'est présentée déjà dans le n° 2

$$F(x) = 30A - 45B - 12(3A - 5B)x$$

qui vérifie les relations

$$\int_0^1 x^2 F(x) dx = A, \quad \int_0^1 x^4 F(x) dx = B.$$

Cette fonction  $F(x)$  décroît de  $M = F(0) = 30A - 45B$  jusqu'à  
 $F(1) = 15B - 6A$ .

On dis maintenant que la valeur  $d = f(1)$  doit être inférieure à  
 $15B - 6A$ . C'est ce qu'on voit facilement en jetant le regard  
sur la Fig. 2, où la fonction  $F(x)$  est représentée par droite FE, et  
en rappelant que la différence  $F(x) - f(x)$  doit changer au moins  
deux fois de signe d'après la proposition du n° 1. Cela se fonde  
sur la notion qu'on a d'une courbe qui tourne sa concavité vers  
le haut car c'est par une telle courbe qu'est représentée la fonction  
 $f(x)$  d'après notre hypothèse. Mais voici une démonstration arith-  
métique. Supposons  $d > D$ , alors  $F(x) - f(x)$  est négative pour  $x = 1$ ,  
comme cette différence doit changer au moins deux fois de signe,  
il doit exister un nombre  $a < 1$  tel que  $F(a) - f(a) > 0$ , et un nombre  
 $b$  tel que  $F(b) - f(b) < 0$ , donc

$$F(1) < f(1),$$

$$F(a) > f(a),$$

$$F(b) < f(b),$$

On tire

$$\frac{F(a) - F(1)}{1 - a} > \frac{f(a) - f(1)}{1 - a}, \quad \frac{F(b) - F(a)}{a - b} < \frac{f(b) - f(a)}{a - b},$$



C

$$\frac{f(b) - f(a)}{a - b} > \frac{f(a) - f(1)}{1 - a},$$

$$\cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \cdot \quad \left\{ \begin{array}{l} 3A > 5B > d, \\ 15B - 6A > d. \end{array} \right.$$

Considérons d'abord les valeurs particulières  $T(0)$ ,  $t(0)$ . La

Fig. 2 fait voir immédiatement que  $T(0)$  n'est autre chose que la valeur de la fonction  $F(x)$ , considérée dans le  $n^0$  précédent pour  $x=0$ , donc

Quant à la valeur de  $t(0)$ , que nous désignerons par  $m$ , on voit sans peine qu'elle correspond à la loi de densité suivante: une densité constante  $m$  de  $x=0$  jusqu'à une certaine valeur

En introduisant  $\Delta$  et  $\lambda$  au lieu de A et B, la limitation  $15 B - 6 A > d$  peut se mettre la forme  $\lambda < \frac{5\Delta}{2\Delta + d}$ . Adoptant les valeurs  $\Delta = 5,56$  et  $d = 2,6$ , il vient  $\lambda < 2,026$ , s'qu'on a  $\lambda = 1,87$ , avec une erreur que j'estime ne pouvoir dépasser notablement 0.06.

411  
 $\rho < 1$ , représentée dans la Fig. 2 par la droite horizontale OD, pour  $x > a$  un décroissement régulier de la densité jusqu'à la surface  $d$  représentée par la droite DB, donc

$$\begin{aligned} f(x) &= m, & 0 < x < a, \\ f(x) &= m - \frac{m-d}{1-a} (x-a), & a < x < 1. \end{aligned}$$

mais il faut faire voir qu'on obtient une détermination convenable de ces deux inconnues  $m$  et  $a$  par les équations (1) et (2). Or on obtient, après quelques réductions qui se présentent d'elles-mêmes

$$\begin{aligned} 12 A - 4 d &= (1+a)(1+a^2)(m-d), \\ 30 B - 6 d &= (1+a)(1+a^2+a^4)(m-d), \end{aligned}$$

pour la détermination de  $a$

$$\dots \dots \dots \frac{1+a^2+a^4}{1+a^2} = \frac{15 B - 3 d}{6 A - 2 d} = \frac{3(5 B - d)}{2(3 A - d)}.$$

Le membre tout connu est supérieur à l'unité mais inférieur à  $\frac{3}{2}$  d'après les inégalités (14), tandis qu'on voit facilement que l'expression  $\frac{1+a^2+a^4}{1+a^2}$  varie de 1 à  $\frac{3}{2}$ , en croissant constamment, quand  $a$  varie de 0 à 1. Donc l'équation (16) détermine une valeur unique de  $a$ , comprise entre 0 et 1.

Après avoir calculé  $a$ , on trouve  $m$  à l'aide de

$$\dots \dots \dots m = d + \frac{12 A - 4 d}{(1+a)(1+a^2)},$$

car, à cause de  $a < 1$  on voit que  $m > 3 A$ , c. à d.  $m$  est supérieur à la densité moyenne de la terre, ce qui est évident a priori.

Voici maintenant comment on obtient la valeur de  $T(b)$  pour une valeur quelconque de  $b$ . Supposons d'abord  $b$  comprise entre 0 et la valeur  $a$  déterminée dans le n<sup>o</sup> précédent.

On a

$$\begin{aligned} F(x) &= K, & 0 < x < b, \\ F(x) &= K - h(x-b), & b < x < 1 \end{aligned}$$

On détermine les constantes  $K, h$  par les conditions (3).

On obtient

$$K = \frac{6(5 - 6b + b^6)A - 15(3 - 4b + b^4)B}{1 - 3b^4 + 2b^6},$$

$$h = \frac{36A - 60B}{1 - 3b^4 + 2b^6}.$$

Dans la Fig. 2 cette fonction  $F(x)$  est représentée par la ligne brisée  $IG$ , et l'on trouve

$$F(1) = AG = \frac{15(1 + b^2)B - 6(1 + b^2 + b^4)A}{1 + b^2 - 2b^4}.$$

Comme on voit,  $h$  est positif et croît avec  $b$ . Quant à la valeur de  $F(1)$ , elle décroît avec  $b$ . C'est ce qui résulte de l'expression

$$F(1) = \frac{5B - 3pA}{1 - p} = 3A - \frac{3A - 5B}{1 - p},$$

car  $p = \frac{2(1 + b^2 + b^4)}{3(1 + b^2)}$  est une fonction croissante.

De ce que  $h$  croît et  $F(1)$  décroît avec  $b$  on peut conclure, d'après la proposition du n° 1, que  $K$  est décroissant. On pourrait aussi s'en convaincre directement.

Il est évident maintenant que pour  $b=0$  la droite  $IG$  se confond avec  $FE$ , et pour  $b=a$  elle se confond avec  $DB$ . Le point  $G$  se situe donc de  $E$  vers  $B$ , en sorte que  $F(1)$  ne devient pas inférieur à  $d$ . On voit maintenant immédiatement qu'il ne peut exister une loi de densité qui donne pour  $x=b$  une densité supérieure à  $K$ ; donc  $F(b) = K$ , c. à d.

$$T(b) = \frac{6(5 - 6b + b^6)A - 15(3 - 4b + b^4)B}{1 - 3b^4 + 2b^6}, \quad 0 \leq b \leq a.$$

Comme on le voit  $T(a) = m$ .

L'équation de la droite  $IG$  est

$$\left\{ \begin{array}{l} y = K - h(x - b), \\ K = \frac{6(5 - 6b + b^6)A - 15(3 - 4b + b^4)B}{1 - 3b^4 + 2b^6}, \\ h = \frac{36A - 60B}{1 - 3b^4 + 2b^6}. \end{array} \right. \quad \text{où}$$

le système de droites IG qu'on obtient en faisant varier  $b$  de 0 à 1 sera appelé le premier système de droites.

Supposons maintenant  $a < b < 1$ , et déterminons une loi de densité  $f(x)$  ainsi

$$f(x) = K - h(x - b), \quad 0 < x < b,$$

$$f(x) = \frac{1}{1-b} [K - db - (K - d, x)], \quad b < x < 1,$$

représentée par la ligne brisée KLB de la fig. 2.

En déterminant  $K$ ,  $h$  par les conditions (1), (2), on trouve

$$K = \frac{30B - 12b^2A - (5 - b - 4b^2)d}{1 + b},$$

$$h = \frac{12(1 + b^2 + b^4)A - 30(1 + b^2)B + 2(1 + b^2 - 2b^4)d}{b^4}.$$

La valeur de  $K$  décroît avec  $b$ , comme on le voit en écrivant

$$K = d + \frac{(30B - 6d) - b^2(12A - 4d)}{1 + b}.$$

Au contraire, en observant que

$$h = 12A - 4d - \frac{2(15B - 6A - d)}{q - 1},$$

et que  $q = \frac{1 + b^2 + b^4}{1 + b^2}$  est une fonction croissante, on voit que la valeur de  $h$  croît avec  $b$ .

Il est évident maintenant que pour  $b = a$  la droite KL se confond avec CD et  $h = 0$ . Pour des valeurs plus grandes de  $b$ ,  $h$  est donc positif, et lorsque  $b = 1$  la droite KL se confond avec FE.

Il est facile de s'assurer qu'il ne peut exister aucune loi de densité qui donne pour  $x = b$  une densité supérieure à  $K$ , donc

$$\dots T(b) = \frac{30B - 12b^2A - (5 - b - 4b^2)d}{1 + b}, \quad a \leq b < 1.$$

fonction  $T(b)$  est maintenant parfaitement connue; remarquons qu'elle présente une discontinuité: en effet,  $\varepsilon$  étant infiniment petit,

$$T(1 - \varepsilon) = 15 B - 6 A > d,$$

$$T(1) = d.$$

représentant la fonction  $T(b)$  par une courbe, cette courbe se compose de deux arcs qui se rencontrent en D, où ils ont des tangentes distinctes. La tangente en F se confond avec la droite FE. Les deux arcs sont convexes vers OA.

L'équation de la droite KL est

$$\begin{cases} y = K - h(x - b), \\ K = \frac{30 B - 12 b^2 A - (5 - b - 4 b^2) d}{1 + b}, \\ h = \frac{12(1 + b^2 + b^4) A - 30(1 + b^2) B + 2(1 + b^2 - 2 b^4) d}{b^4}. \end{cases} \quad \text{où}$$

le système des droites KL qu'on obtient en faisant varier  $b$  de 0 à 1 sera appelé le second système de droites. On verra facilement que l'intersection K se meut toujours dans le même sens de C vers F.

Il nous reste à déterminer la fonction  $t(b)$ , dont jusqu'à présent nous connaissons seulement les valeurs particulières  $t(0) = m$ ,  $t(1) = d$ . Or cela ne semble pas possible d'une manière aussi directe que celle qui nous a fait trouver la valeur de  $T(b)$ . On verra aussi que l'expression analytique de  $t(b)$  est beaucoup plus compliquée que celle de  $T(b)$ .

Supposons que dans la Fig. 2 on ait tracé les droites du premier et du second système. Ces droites occupent, dans leur ensemble, une certaine partie du plan, limitée inférieurement par une certaine courbe. Nous allons déterminer cette courbe, mais, pour motiver la recherche qui pourrait sembler étrangère à notre objet, disons tout d'abord que cette courbe n'est autre chose que la représentation géométrique de la fonction  $t(b)$ .

Enfin, nous sommes amenés ainsi à la recherche des courbes limites des deux systèmes de droites.

*Courbe enveloppe du premier système de droites.*

L'équation d'une droite du premier système a déjà été donnée, (19). Pour avoir l'enveloppe, il faut prendre la dérivée par rapport à  $b$  et éliminer ensuite ce paramètre entre l'équation obtenue et l'équation primitive. On obtiendrait ainsi l'équation de la courbe enveloppe, mais cela serait de peu d'importance pour le sujet, et il est bien plus naturel d'exprimer seulement les coordonnées  $x, y$  de la courbe par le paramètre  $b$ , dont on connaît la signification. Les équations étant linéaires en  $x$  et  $y$ , ce calcul présente aucune difficulté et l'on obtient

$$\left\{ \begin{array}{l} x = \frac{10 + b^2 + b^4}{12}, \\ y = \frac{5B - 3b^2A}{1 - b^2}. \end{array} \right. \quad 0 \leq b \leq a,$$

Il est remarquable que l'expression de  $x$  ne contient ni  $A$ , ni  $B$ . On obtient les extrémités  $P, Q$  de l'arc courbe, situées sur les droites  $AD, DB$ , en posant  $b=0$  et  $b=a$ . L'abscisse du point  $P$  est donc celle de  $Q$  est  $= \frac{10 + a^2 + a^4}{12}$  et par conséquent inférieure à l'unité.

*Courbe enveloppe du second système de droites.* On peut suivre la même méthode pour obtenir cette seconde courbe, en partant de l'équation (21). On obtient par un calcul un peu laborieux, mais qui ne présente aucune difficulté

$$\left\{ \begin{array}{l} (1+b)^2(4+2b^2)x = 3b + 6b^2 + 4b^3 + 2b^4, \\ b^3(1+b)^2(4+2b^2)y = \\ = 12(1+2b+3b^2+4b^3+5b^4)A - 30(1+2b+3b^2)B + \\ + 2(1+b)(1-b)^2(1+3b+7b^2+3b^3+b^4)d. \end{array} \right. \quad a \leq b \leq 1$$

Ici encore l'expression de  $x$  ne contient point les données  $A, B, d$ . On obtient les extrémités  $R, S$  de l'arc courbe, situées sur les droites  $CD, FE$ , en posant  $b=a$  et  $b=1$ . L'abscisse du point  $R$  est la même, celle de  $S$  est  $\frac{5}{6}$ .

D'après cela, la limite inférieure de la partie du plan occupée par les droites du premier et du second système se compose des 5 parties suivantes:

- 1<sup>o</sup> la droite horizontale CR,
- 2<sup>o</sup> l'arc courbe RS,
- 3<sup>o</sup> la droite inclinée SP,
- 4<sup>o</sup> l'arc courbe PQ,
- 5<sup>o</sup> la droite inclinée QB.

us allons faire voir maintenant que cette ligne CRSPQB est  
 ment la représentation géométrique de la fonction cherchée  
 supposons qu'on trace la ligne  $y=f(x)$  et nommons cette ligne  
 courbe de densité. Alors nous devons montrer qu'aucune courbe  
 densité n'est possible qui pénètre dans la partie du plan au-dessous  
 CRSPQB.

Voici d'abord quelques observations préliminaires:

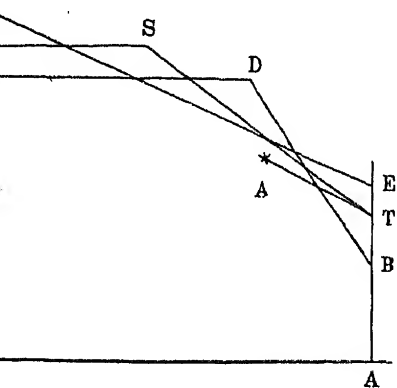
Une courbe de densité (qui commence toujours en B), ne peut  
 en B une inclinaison plus faible sur l'axe OA que la ligne BD.  
 est évident parce qu'elle doit couper en deux points la ligne  
 CDB, d'après la proposition du n<sup>o</sup> 1.

Toute courbe de densité doit couper en deux points la droite

suivant une courbe de densité de B vers l'axe OY, l'inclinaison  
 tangente sur OA va toujours en diminuant, d'après notre hypo-

Il est évident par là que l'inclinaison de cette tangente sur-  
 celle de EF pour la partie de la courbe entre B et la première

Fig. 3.



intersection avec EF, tandis que  
 l'inclinaison de la tangente est  
 plus faible que celle de EF pour  
 la partie de la courbe entre le  
 second point d'intersection avec  
 EF et l'axe OY.

Supposons maintenant qu'il  
 existe une courbe de densité  
 dont un point A est situé au-  
 dessous de la courbe CRSPQB.

Je distingue deux cas:

Le point A se trouve entre B et la première intersection de  
 rbe avec EF. (Fig. 3).

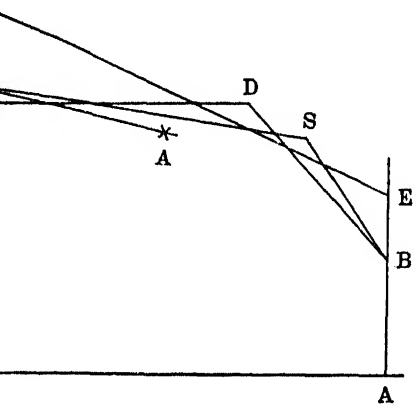
Alors la tangente en A doit couper la ligne BE dans un point T au-dessous de E parce que l'inclinaison de la tangente est plus forte que celle de EF. Mais ce point T doit se trouver au-dessus de B et peut se confondre avec B, car dans ce dernier cas la courbe de densité entre A et B devrait se confondre avec sa tangente AB, ce qui est impossible d'après (A).

Maintenant par le point T passe une droite du premier système qu'on peut compléter par une droite horizontale SU de manière d'obtenir une ligne brisée TSU, représentation d'une fonction  $F(x)$  qui satisfait aux conditions (3)<sup>1</sup>.

La courbe de densité se trouve située entièrement au-dessous de la tangente TA, par conséquent elle ne peut couper la droite TSU. Quant à la droite horizontale SU, elle ne peut la couper qu'en un seul point. Mais, d'après la proposition du n° 1, chaque courbe de densité doit avoir au moins deux intersections avec TSU, par conséquent il ne peut exister une courbe de densité avec le point A au-dessous de CRSPQB.

Le point A se trouve entre la seconde intersection de la courbe de densité avec EF et l'axe OY

Fig. 4.



(Fig. 4). Alors la tangente en A doit couper OY en un point T au-dessous de F, parce que l'inclinaison de cette tangente sur OX est plus faible que celle de EF. Le point T se trouve naturellement au-dessus de C, parce que la courbe elle-même vient rencontrer l'axe OY au-dessus de C.

Maintenant il passe par T une droite TS du second système, et joignant S et B par une droite, on peut regarder TSB comme une courbe de densité. Mais évidemment

La droite TS doit avoir naturellement une inclinaison sur OX plus forte que celle de EF, parce qu'on suppose que A se trouve dans la partie du plan au-dessous de la courbe de densité des droites du premier système.



Et la courbe de densité passant par A ne peut couper la droite, et l'on se trouve de nouveau en contradiction avec la proposition du n° 1.

En somme il ne peut exister aucune courbe de densité qui pénètre dans la partie du plan au-dessous de CRSPQB et cette courbe est, comme nous l'avons annoncé, la représentation géométrique de la fonction  $t(b)$ .

Voici maintenant la détermination analytique de la fonction  $t(b)$ .

Posons  $x_1, x_2, x_3, x_4$  les abscisses des points R, S, P, Q :

$$x_1 = \frac{3a + 6a^2 + 4a^3 + 2a^4}{(1+a)^3(4+2a^2)}, \quad x_2 = \frac{5}{8}, \quad x_3 = \frac{5}{6}, \quad x_4 = \frac{10 + a^2 + a^4}{12}.$$

Alors on a

$$t(b) = m, \quad 0 \leq b \leq x_1.$$

Et lorsque  $b$  est comprise entre  $x_1$  et  $x_2$ , il faut d'abord calculer la quantité  $u$  comprise entre  $a$  et 1 à l'aide de l'équation du 4<sup>ème</sup> degré

$$(1+u)^2(4+2u^2)b = 3u + 6u^2 + 4u^3 + 2u^4,$$

on obtient  $t(b)$  à l'aide de l'équation

$$u^3(1+u)^2(4+2u^2)t(b) = 12(1+2u+3u^2+4u^3+5u^4)A - 30(1+2u+3u^2)B + 2(1+u)(1-u)^2(1+3u+7u^2+3u^3+u^4)d.$$

et ensuite

$$t(b) = 30A - 45B - 12(3A - 5B)b, \quad x_2 \leq b \leq x_3.$$

Dans le quatrième intervalle  $x_3 \leq b \leq x_4$ , il faut calculer la quantité  $u$  comprise entre 0 et  $a$  à l'aide de

$$b = \frac{10 + u^2 + u^4}{12},$$

ensuite on a

$$t(b) = \frac{5B - 3u^2A}{1-u^2}.$$

Enfin, dans le dernier intervalle  $x_4 \leq b \leq 1$ , on a

$$t(b) = m - \frac{m-d}{1-a}(b-a).$$

j'avais d'abord considéré seulement les limites de la densité au centre de la terre, dans les deux hypothèses que nous venons de discuter complètement. En causant sur les résultats obtenus avec Bakhuyzen, celui-ci me suggéra l'idée de chercher des limites de la densité dans un point quelconque de l'intérieur de la terre. Je suis aperçu alors que ma méthode donnait encore facilement la solution de ce problème plus général.

### TROISIÈME PARTIE.

Pour la réduction en nombres des résultats obtenus par la suppression de l'hypothèse II, j'adopterai les valeurs  $d = 2.6$ ,  $\Delta = 5.56$ , le dernier nombre étant celui donné par MM. Cornu et Baillet-Latour [Comptes Rendus de l'Acad. d. Sc., Tome 76]. Quant à  $\lambda$ , cette constante est déterminée par la relation

$$\lambda = \frac{\frac{C - A}{C}}{\varepsilon - \frac{1}{2}\varphi},$$

A étant les moments d'inertie de la terre par rapport à l'axe de rotation et à un diamètre quelconque de l'équateur,  $\varepsilon$  l'aplatissement de la terre,  $\varphi$  le rapport de la force centrifuge à la pesanteur à l'équateur. J'ai adopté la valeur

$$\frac{C - A}{C} = 0.00324256 \text{ } ^1)$$

obtenue par M. Nyren dans son Mémoire sur la détermination de la rotation de l'axe terrestre. [Mém. de l'Acad. Impér. de St. Pétersb., 2<sup>e</sup> Série, Tome XIX].

Quant à  $\varepsilon$  et  $\varphi$ , j'ai adopté les valeurs déduites par M. Listing [Abhandl. der Königl. Ges. d. Wiss. zu Göttingen, 1877)

$$\varepsilon = 0.003466445 = 1 : 288.4800,$$

$$\varphi = 0.003467199 = 1 : 288.4179.$$

---

<sup>1)</sup> La légère différence entre ce nombre et celui qu'on trouve à la page 19 du Mémoire de M. Nyren s'explique par la Note qu'on trouve à la page 54.

en déduit  $\lambda = 1.8712$ , mais j'ai adopté simplement

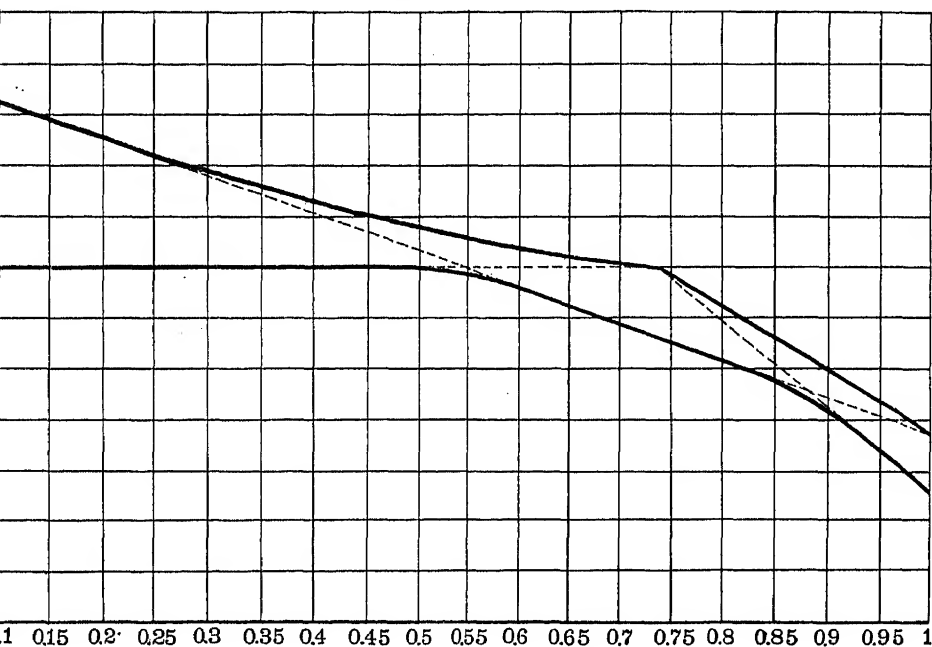
$$\lambda = 1.87.$$

nombre est certainement sujet à quelque incertitude; il me e pourtant difficile d'admettre que l'erreur surpasse notable-0.06. J'ai donc calculé quelques valeurs numériques des fonc- $T(b)$  et  $t(b)$  en adoptant les valeurs

$$d = 2.6, \Delta = 5.56, \lambda = 1.87,$$

comme une faible variation de  $\lambda$  a une influence notable sur résultats, j'ai encore repris le même calcul avec la valeur 0.2.

Fig. 5.



ci maintenant les valeurs obtenues; la Fig. 5 donne la représentation graphique correspondant à la valeur  $\lambda = 1.87$

$$\lambda = 1.87, \alpha = 0.73985, m = 6.998, M = 11.001, D = 3.746.$$

$$\lambda = 1.92, \alpha = 0.65416, m = 7.613, M = 12.162, D = 3.359.$$

$$\lambda = 1.87, x_1 = 0.50077, x_2 = \frac{5}{8}, x_3 = \frac{5}{8}, x_4 = 0.90392,$$

$$\lambda = 1.92, x_1 = 0.45278, x_2 = \frac{5}{8}, x_3 = \frac{5}{8}, x_4 = 0.88425.$$

$\lambda = 1.87$		$\lambda = 1.92$		
T (b)	t (b)	T (b)	t (b)	
11.00	7.00	12.16	7.61	
10.64	7.00	11.72	7.61	
10.28	7.00	11.28	7.61	
9.92	7.00	10.85	7.61	
9.57	7.00	10.43	7.61	
9.24	7.00	10.02	7.61	
8.92	7.00	9.63	7.61	
8.62	7.00	9.27	7.61	
8.34	7.00	8.93	7.61	
8.08	7.00	8.62	7.61	
7.84	7.00	8.33	7.51	
7.63	6.90	8.07	7.24	
7.44	6.64	7.84	6.87	
7.27	6.29	7.63	6.44	
7.11	5.92	7.05	6.00	
6.87	5.56	6.43	5.56	
6.24	5.20	5.81	5.12	
5.62	4.83	5.20	4.68	
4.99	4.29	4.58	4.05	
4.37	3.45	3.97	3.32	
2.60 (3.75)	2.60	2.60 (3.36)	2.60	

Newton, en considérant la terre comme une masse fluide homogène, douée d'un mouvement de rotation, et en supposant la forme propre à l'équilibre est celle d'un ellipsoïde de révolution, a déterminé le rapport des axes du globe terrestre. En nommant  $\varphi$  le rapport de la force centrifuge à la pesanteur à l'équateur, il trouve l'aplatissement égal à  $\frac{5}{4} \varphi$ . Clairaut, dans sa „Théorie de la figure de la terre”, a confirmé ce résultat; et, en abandonnant l'hypothèse de l'homogénéité, il a trouvé pour la première fois le moyen de déterminer l'aplatissement en supposant donnée la loi de la variation de la densité. En sup-

et que la densité croît constamment à mesure qu'on s'approche du centre de la terre, il arrive à ce résultat que l'aplatissement est plus faible que dans l'hypothèse de l'homogénéité.

Enfin, plus tard, les observations avaient montré d'une manière évidente que l'aplatissement du globe terrestre est, en effet, plus grand que dans l'hypothèse d'une densité constante, il était naturel de proposer une loi de densité propre à donner l'aplatissement observé.

Il paraît que la première hypothèse proposée est celle de Legendre, que Laplace a discutée plus tard dans la Mécanique céleste; elle conduit à supposer

$$f(x) = C \frac{\sin nx}{x}.$$

On en déduit aisément

$$\Delta = 3 \int_0^1 x^2 f(x) dx = 3C \frac{\sin n - n \cos n}{n^2},$$

$$\lambda = \frac{\int_0^1 x^2 f(x) dx}{\int_0^1 x^4 f(x) dx} = \frac{n^2 (\sin n - n \cos n)}{(3n^2 - 6) \sin n - (n^3 - 6n) \cos n},$$

$$d = C \sin n.$$

D'après la théorie de Clairaut, l'aplatissement  $\varepsilon$  se détermine à l'aide de

$$\varepsilon = \frac{5}{2} \varphi \cdot \frac{\frac{3(1 - n \cotg n)}{n^2} - 1}{\frac{n^2}{1 - n \cotg n} - 2 - n \cotg n}.$$

En adoptant la valeur  $\Delta = 5.56$  et la valeur de  $\varphi$  donnée précédemment d'après Listing, j'ai calculé les valeurs de  $d$ ,  $\lambda$ ,  $\varepsilon$  pour diverses valeurs de  $n$ ; — voici les résultats :

## Hypothèse de Legendre.

$n$	$d$	$\lambda$	$\varepsilon$
136°	3.02	1.948	1 : 286.3
137	2.97	1.954	1 : 287.5
138	2.93	1.961	1 : 288.7
139	2.88	1.968	1 : 290.0
140	2.83	1.975	1 : 291.3
141	2.78	1.982	1 : 292.6
142	2.73	1.990	1 : 294.0
143	2.68	1.998	1 : 295.4
144	2.63	2.006	1 : 296.8
145	2.57	2.014	1 : 298.2
146	2.52	2.022	1 : 299.7

Comme on le voit, l'hypothèse de Legendre ne peut pas représenter suffisamment les faits observés. Dans la Mécanique céleste, la place admet la valeur  $n = 150^\circ$ , ce qui répond à la valeur 1 : 306.6 d'aplatissement, qu'on ne peut plus admettre. On voit aussi qu'on obtient ainsi une valeur beaucoup trop forte de  $\lambda$ .

La loi de Legendre  $f(x) = C \frac{\sin nx}{x}$  ne satisfait pas à notre hypothèse II. On trouve que  $f''(x)$  change de signe dans le voisinage de la surface de la terre, en sorte que la courbe de densité présente une inflexion. Toutefois, la convexité vers l'axe  $OA$  est peu sensible. Plus tard M. Roche a proposé la formule  $f(x) = a - bx^2$ , mais je passerai directement à la loi plus générale

$$f(x) = a - bx^n,$$

proposée par M. Lipschitz (Journal de Borchardt, Bd 62).

Dans cette hypothèse, l'équation différentielle du second ordre qui dépend de l'aplatissement peut s'intégrer à l'aide de la fonction hypergéométrique de Gauss. Les trois constantes  $a, b, n$  sont déterminées à l'aide des trois données  $d, \Delta$ , et  $\frac{\varepsilon}{\varphi}$ .

M. Lipschitz obtient une équation transcendante pour l'inconnue  $n$  et démontre par une analyse ingénieuse que cette équation admet

la racine positive. Dès que  $n$  est connu, on obtient  $a$  et  $b$  par les formules

$$a = \frac{(n+3)\Delta - 3d}{n},$$

$$b = \frac{(n+3)(\Delta - d)}{n}.$$

Lipschitz obtient ainsi

$$f(x) = 9.453 - 6.953 x^{3.89},$$

attribuant à  $d$ ,  $\Delta$ ,  $\frac{\varepsilon}{\varphi}$  des valeurs qui diffèrent légèrement de celles que nous avons données plus haut. Comme on le voit, la formule donnée qui n'a pas été employée par M. Lipschitz, c'est la formule (1). On peut donc avoir une vérification en calculant la valeur de  $\lambda$  d'après la formule de M. Lipschitz. J'ai donc calculé la valeur de  $\lambda$  en adoptant la valeur  $\Delta = 5.56$  et les valeurs de  $\varepsilon$  et  $\varphi$  d'après Listing, pour différentes valeurs de  $d$ . J'ai obtenu

$d$	$\lambda$
2.0	1.963
2.2	1.963
2.4	1.963
2.6	1.963
2.8	1.964
3.0	1.964

Comme on le voit, cette valeur de  $\lambda$  est un peu forte et à peu près indépendante de  $d$ . Mais la valeur de  $\lambda$  ne dépend pas des valeurs absolues de  $d$  et  $\Delta$ , mais seulement de leur rapport. On ne peut donc pas obtenir une valeur plus faible de  $\lambda$  en faisant varier  $\Delta$ . Il reste seulement à chercher l'influence de l'aplatissement.

On a pu abréger beaucoup les calculs nécessaires à l'aide d'une formule que M. Tisserand m'a bien voulu me communiquer et que l'on trouvera dans les Comptes Rendus de l'Acad. d. Sciences (tome 13, 1884). Cette formule donne directement une valeur suffisamment approchée

résultats précédents supposent  $\varepsilon = 1 : 288.48$ , mais en posant  $\varepsilon = 1 : 280$ ,  $d = 2.6$  (les autres données restant les mêmes), il vient

$$\lambda = 1.927.$$

Comme on le voit, dans toutes les hypothèses admissibles, on aura toujours une valeur de  $\lambda$  un peu forte. Cela semble indiquer que la densité au centre est encore un peu plus faible et que la diminution de la densité en s'éloignant du centre est encore plus lente, que ne le suppose la loi de M. Lipschitz.

---



# XXXV.

(Bul. astr., Paris, 1, 1884, 568.)

ote sur quelques formules pour l'évaluation de certaines  
intégrales.

semble que des trois formules suivantes

$$\begin{aligned} \int_{-1}^{+1} \frac{f(x)}{\sqrt{1-x^2}} dx &= \int_0^\pi f(\cos \varphi) d\varphi = \frac{\pi}{n} \sum_{k=1}^{k=n} f\left[\cos \frac{(2k-1)\pi}{2n}\right] + \text{corr.}, \\ \left\{ \int_{-1}^{+1} \sqrt{1-x^2} f(x) dx &= \int_0^\pi \sin^2 \varphi f(\cos \varphi) d\varphi \right. \\ &= \frac{\pi}{n+1} \sum_{k=1}^{k=n} \sin^2 \frac{k\pi}{n+1} f\left[\cos \frac{k\pi}{n+1}\right] + \text{corr.}, \\ \left. \int_{-1}^{+1} \sqrt{\frac{1-x}{1+x}} f(x) dx &= 2 \int_0^\pi \sin^2 \frac{1}{2} \varphi f(\cos \varphi) d\varphi \right. \\ &= \frac{4\pi}{2n+1} \sum_{k=1}^{k=n} \sin^2 \frac{k\pi}{2n+1} f\left(\cos \frac{2k\pi}{2n+1}\right) + \text{corr.}, \end{aligned}$$

première (A) seule soit généralement connue. La correction est  
lorsque  $f(x)$  est un polynôme en  $x$  du degré  $2n-1$  au plus.  
On peut encore écrire ces formules sous la forme suivante

$$\begin{aligned} \int_0^1 \frac{f(x)}{\sqrt{x(1-x)}} dx &= \frac{\pi}{n} \sum_{k=1}^{k=n} f\left[\cos^2 \frac{(2k-1)\pi}{4n}\right] + \text{corr.}, \\ \int_0^1 \sqrt{x(1-x)} f(x) dx &= \frac{\pi}{4n+4} \sum_{k=1}^{k=n} \sin^2 \frac{k\pi}{n+1} f\left(\cos^2 \frac{k\pi}{2n+2}\right) + \text{corr.}, \\ \int_0^1 \sqrt{\frac{1-x}{x}} f(x) dx &= \frac{2\pi}{2n+1} \sum_{k=1}^{k=n} \sin^2 \frac{k\pi}{2n+1} f\left(\cos^2 \frac{k\pi}{2n+1}\right) + \text{corr.} \end{aligned}$$

Pour donner une application, prenons l'intégrale

$$Y = \int_0^1 \sqrt{x(1-x)(1+kx)} dx,$$

rencontrée récemment par M. Seeliger dans une question relative à l'anneau de Saturne (Astron. Nachr., n° 2612), la constante  $k$  étant inférieure à l'unité. Lorsque  $k=1$ , la valeur exacte de  $Y$  est

$$0,47925609389423688 \dots$$

En posant maintenant  $f(x) = \sqrt{1+x}$  dans la formule (B<sub>1</sub>), on trouve

$$n=1, \quad \text{corr.} = -0,0017,$$

$$n=2, \quad \text{corr.} = -0,000015,$$

$$n=3, \quad \text{corr.} = -0,00000024,$$

$$n=5, \quad \text{corr.} = -0,000000000080.$$

Lorsque  $k$  est une fraction, les corrections sont encore plus petites; en prenant  $n=2$ , on a donc

$$Y = \frac{\pi}{16} (\sqrt{1+\frac{1}{4}k} + \sqrt{1+\frac{3}{4}k}),$$

avec une erreur moindre que deux unités de la cinquième décimale.

XXXVI.

(Paris, C.-R. Acad. Sci., 99, 1884, 850—851.)

Sur une généralisation de la théorie des quadratures  
mécaniques.

(Note, présentée par M. Tisserand.)

soit  $f(x)$  une fonction qui ne devient pas négative, dans l'intervalle  $0 \leq x \leq 1$ , et soit  $\lambda_1, \lambda_2, \dots, \lambda_n$  des nombres positifs inégaux, tels que  $\lambda_1 + \lambda_2 + \dots + \lambda_n = 1$ ; lorsque  $n$  est pair, égal à  $2m$ , le système des  $2m$  équations

[illegible]

et une solution par des nombres positifs  $A_1, A_2, \dots, A_m$  et des valeurs de  $x_1, x_2, \dots, x_m$  qui sont positives, inégales et inférieures à l'unité. Cette solution est unique, en faisant abstraction des permutations qu'on peut effectuer simultanément sur les quantités  $A_1, \dots, A_m$  et  $x_1, x_2, \dots, x_m$ .

De même, lorsque  $n = 2m + 1$ , le système des équations

$$\dots \alpha_k = A_1 x_1^{\lambda_k} + A_2 x_2^{\lambda_k} + \dots + A_m x_m^{\lambda_k} + A_{m+1},$$

et prend les valeurs  $1, 2, \dots, n$ , admet une solution unique,  $x_1, \dots, x_m$  étant positifs, inégaux et inférieurs à l'unité,  $A_1, A_2, \dots, A_{m+1}$  étant positifs.

Lorsque  $n$  est pair et qu'on prend  $\lambda_k = k - 1$ , on se trouve dans le cas des quadratures mécaniques.

Voici maintenant une interprétation quasi mécanique des formules (1), en supposant qu'aucun des nombres  $\lambda_k$  ne soit égal à zéro. Soit  $OA$  une droite de longueur égale à 1. En attribuant à cette droite une densité  $f(x)$  à la distance  $x$  de l'origine  $O$ , on peut considérer les moments  $a_1, a_2, \dots, a_n$  comme des moments par rapport à l'origine  $O$ . Supposons maintenant qu'on fasse varier la distribution de la masse, de telle manière que les moments  $a_1, a_2, \dots, a_n$  restent constants. Dans ces conditions, il existe évidemment un minimum de la masse totale. Ce minimum se présente lorsqu'on place des masses finies  $A_1, A_2, \dots, A_m$  à des distances  $x_1, x_2, \dots, x_m$  de l'origine  $O$ , et les équations (1) expriment alors simplement que les conditions imposées aux moments se trouvent vérifiées.

Nous avons dit que, dans les formules (1),  $x_1, x_2, \dots, x_m$  sont quelconques; mais, dans un cas spécial, il peut y avoir égalité entre quelques-uns de ces nombres. Cela n'arrive toutefois que, quand la distribution primitive de masse, qui a servi à calculer  $a_1, a_2, \dots, a_n$ , consiste en une concentration de masses finies dans un nombre de points de  $OA$  inférieur à  $m$ . Alors cette distribution primitive correspond déjà au minimum. On peut aussi se figurer que, dans ce cas, quelques-unes des quantités  $A_1, A_2, \dots, A_m$  s'évanouissent.

Les équations (2) admettent une interprétation semblable: la masse  $A_{m+1}$  se trouve alors à l'extrémité  $A$  de la droite.

D'après ce qui précède, on a, dans les deux cas,

$$A_1 + A_2 + \dots + A_m \leq \int_0^1 f(x) dx,$$

$$A_1 + A_2 + \dots + A_{m+1} \leq \int_0^1 f(x) dx.$$

## XXXVII.

Ann. Sci. Éc. norm., Paris, sér. 3, 2, 1885, 183—184.)

---

note à l'occasion de la réclamation de M. Markoff<sup>1</sup>).

En réponse à la réclamation de M. Markoff, je dois déclarer que c'est par lui que j'ai appris l'existence de l'article de M. Tchebychev sur les valeurs limites des intégrales (Journal de Liouville, 1874), et que j'ai trouvé déjà l'énoncé des inégalités en question. Je regrette bien de n'avoir pas connu plus tôt ce travail.

Mon travail, mes recherches ont été tout à fait indépendantes de celles de M. Tchebychev et Markoff: en effet, mon travail a été remis à la Commission des Annales de l'École Normale vers le milieu du mois de septembre 1884, et je viens d'apprendre que la livraison des Mathematische Annalen contenant l'article de M. Markoff n'est arrivée ici à la bibliothèque de l'Université que dans la seconde moitié de septembre 1884. Naturellement, je reconnais volontiers que M. Markoff a, le premier, donné une démonstration des inégalités de M. Tchebychev. Je veux profiter de cette occasion pour ajouter une remarque nouvelle sur le sujet traité dans mon Mémoire.

La démonstration des inégalités de M. Tchebychev en forme bien une partie essentielle; mais, pour le but que je me suis proposé, il n'est pas moins essentiel de démontrer que les  $A_k$  convergent vers zéro. Ce point important, je l'ai démontré d'une manière indirecte en m'appuyant sur le développement d'une fonction arbitraire par

---

<sup>1</sup> La réclamation concerne le mémoire: Quelques recherches sur la théorie des quadratures mécaniques, N° XXXI.

série de Fourier. Il semble pourtant très désirable d'établir cela d'une manière plus simple et plus directe, mais mes efforts dans cette direction n'ont pas conduit au but désiré.

On peut voir, dans une Note que j'ai présentée à l'Académie des Sciences et qui se trouve dans les Comptes rendus du 22 septembre 1884, que la question à laquelle je touche ici a une liaison intime avec la convergence d'une certaine fraction continue.

Voici maintenant une propriété nouvelle des coefficients  $A_k$  que j'ai découverte dans cette recherche.

Pour mettre en évidence la dépendance de  $A_1, A_2, \dots, A_k, \dots$ , du nombre entier  $n$ , je désignerai maintenant ces nombres par  $A_1^n, A_2^n, \dots, \dots$ . Avec cette notation, je trouve qu'on a toujours

$$A_1^{n+1} + A_2^{n+1} + \dots + A_k^{n+1} < A_1^n + A_2^n + \dots + A_k^n,$$

$$A_1^{n+1} + A_2^{n+1} + \dots + A_k^{n+1} > A_1^n + A_2^n + \dots + A_{k-1}^n.$$


---

# XXXVIII.

(Acta Math., Stockholm, 6, 1885, 319—320.)

## Un théorème d'algèbre.

(Extrait d'une Lettre adressée à M. Hermite.)

Un théorème d'algèbre qui s'est présenté à moi en étudiant les formules analytiques qui servent à exprimer le déplacement d'un point variable autour d'un point fixe. (Voir Duhamel: Cours de Mécanique, introduction.)

est

$$\begin{vmatrix} a & b & c \\ a' & b' & c' \\ a'' & b'' & c'' \end{vmatrix} \quad \text{et} \quad \begin{vmatrix} A & B & C \\ A' & B' & C' \\ A'' & B'' & C'' \end{vmatrix}$$

coefficients de deux substitutions orthogonales à déterminant  $+1$  et

$$R = \begin{vmatrix} A + a & B + b & C + c \\ A' + a' & B' + b' & C' + c' \\ A'' + a'' & B'' + b'' & C'' + c'' \end{vmatrix}$$

le déterminant  $R$  (qui visiblement n'est pas identiquement zéro) a la propriété que lorsque  $R=0$  en même temps tous ses mineurs du second degré s'évanouissent. Je trouve en effet que le déterminant d'un tel mineur peut se mettre sous la forme

$$R \times \text{Fonction entière de } a, \dots, c'', A, \dots, C''.$$

La signification géométrique de ce théorème. Lorsque, par l'effet d'un déplacement, un seul point  $(x, y, z)$  vient dans la position  $(-x, -y, -z)$  cela entraîne nécessairement que tous les points d'un certain système partagent de la même propriété. Le déplacement se ramène à une rotation de  $180^\circ$  autour d'un certain axe. C'est du reste un cas d'ex-

ception qui échappe à l'analyse de M. Duhamel. Les formules de M. Duhamel cessent de déterminer l'axe de rotation (qui pourtant est parfaitement déterminé) parce qu'on a  $p=0$ ,  $q=0$ ,  $r=0$ . (On a  $p^2 + q^2 + r^2 = \sin^2 \omega$  dans la notation de M. Duhamel.)

Ce théorème d'algèbre subsiste encore dans le cas de deux variables

$$\begin{vmatrix} a & b \\ a' & b' \end{vmatrix}, \quad \begin{vmatrix} A & B \\ A' & B' \end{vmatrix}$$

et j'ai lieu de penser qu'il en est de même pour quatre variables, bien que je ne l'aie pas encore complètement démontré. Serait-il donc possible de l'étendre à un nombre quelconque de variables? Ce sujet a quelque rapport au théorème de M. Brioschi, que l'équation

$$\begin{vmatrix} a+z & b & c & \dots & k \\ a' & b'+z & c' & \dots & k' \\ a'' & b'' & c''+z & \dots & k'' \\ \dots & \dots & \dots & \dots & \dots \\ a^{(n-1)} & b^{(n-1)} & c^{(n-1)} & \dots & k^{(n-1)}+z \end{vmatrix} = 0$$

ses racines réciproques et imaginaires (abstraction faite de la racine  $= -1$  lorsque  $n$  est impair)<sup>1)</sup>.

<sup>1)</sup> Journ. de Liouville, t. 19. 1e sér. p. 253.



# XXXIX.

(Acta Math., Stockholm, 6, 1885, 321—326.)

certaines polynômes qui vérifient une équation différentielle  
linéaire du second ordre et sur la théorie des  
fonctions de Lamé.

Dans les Comptes rendus de l'Académie des sciences de Berlin, 1864 (et dans son *Traité des fonctions sphériques*, tome I, p. s., 2<sup>de</sup> édit.) M. Heine a démontré la proposition suivante. Soient A et B deux polynômes donnés en  $x$ , le premier du degré  $p$ , le second du degré  $p$  au plus, ces polynômes étant d'ailleurs quelconques, le fait généraux et n'étant assujettis à aucune condition, et considérons l'équation différentielle

$$\dots \dots \dots A \frac{d^2 y}{dx^2} + 2 B \frac{dy}{dx} + C y = 0$$

est un polynôme en  $x$  du degré  $p - 1$  au plus.

Il existe toujours certaines déterminations particulières du polynôme C, telles que l'équation (1) admette comme intégrale un polynôme en  $x$  du degré  $n$ . Le nombre de ces déterminations et des polynômes correspondants  $y$  s'élève à

$$(n, p) = \frac{(n+1)(n+2)(n+3) \dots (n+p-1)}{1 \cdot 2 \cdot 3 \dots (p-1)}$$

$$(n, 1) = 1.$$

Ce théorème constitue le fondement principal de la théorie générale

es fonctions de Lamé qu'on doit à M. Heine. Dans cette théorie la fonction B n'est pas indépendante de A, car l'on a  $B = \frac{1}{4} \frac{dA}{dx}$ . M. Heine voit que la détermination du polynôme C dépend d'un système d'équations algébriques de degrés supérieurs et que l'équation finale qu'on obtient en éliminant toutes les inconnues sauf une, est au plus du degré  $(n.p)$ . En outre on voit qu'à chaque détermination de C correspond un polynôme déterminé  $y$  du degré  $n$ .

Mais on voit moins facilement que le degré de l'équation finale d'où dépend le polynôme C atteint effectivement le degré  $(n.p)$ . M. Heine a levé cette difficulté en faisant voir par un calcul de proche en proche que, même en soumettant les polynômes A et B à certaines conditions particulières, il existe effectivement  $(n.p)$  polynômes du degré  $n$  qui satisfont à une équation différentielle de la forme (1).

Je me propose de démontrer, dans ce qui suit, la proposition suivante. Lorsque les racines  $\alpha_0, \alpha_1, \alpha_2, \dots, \alpha_p$  de l'équation  $A = 0$  sont réelles et inégales et qu'en posant

$$\frac{B}{A} = \frac{\alpha_0}{x - \alpha_0} + \frac{\alpha_1}{x - \alpha_1} + \dots + \frac{\alpha_p}{x - \alpha_p}$$

les quantités  $\alpha_0, \alpha_1, \dots, \alpha_p$  sont positives, alors les  $(n.p)$  déterminations du polynôme C sont toutes réelles ainsi que les polynômes correspondants  $y$  du degré  $n$ . Soit  $y_1$  un de ces derniers polynômes, les racines de  $y_1 = 0$  sont réelles et inégales et distribuées dans les  $p$  intervalles des racines de  $A = 0$ .

Le nombre des manières dont on peut distribuer  $n$  quantités dans  $p$  intervalles est évidemment égal à  $(n.p)$  et j'ajoute maintenant que les racines des polynômes  $y$  représentent en effet toutes ces distributions, en sorte qu'un tel polynôme est parfaitement caractérisé par la distribution de ses  $n$  racines dans les  $p$  intervalles des racines  $\alpha_0, \alpha_1, \dots, \alpha_p$  de  $A = 0$ .

2. Soient, sur un axe  $OX$ ,  $A_0, A_1, A_2, \dots, A_p$  les points dont les abscisses sont  $\alpha_0, \alpha_1, \dots, \alpha_p$  et prenons encore, dans un quelconque des  $p$  intervalles déterminés par ces points (p. e.  $(A_0, A_1)$ ),  $n$  points  $X_1, X_2, \dots, X_n$  dont les abscisses sont  $x_1, x_2, \dots, x_n$ . Cela posé,



J'observe maintenant qu'on a d'après (2)

$$\frac{a_0}{x_k - a_0} + \frac{a_1}{x_k - a_1} + \dots + \frac{a_p}{x_k - a_p} = \frac{B(x_k)}{A(x_k)}$$

en posant

$$y = (x - x_1)(x - x_2) \dots (x - x_n)$$

il vient

$$\frac{y'}{y} - \frac{1}{x - x_k} = \frac{1}{x - x_1} + \dots + \frac{1}{x - x_{k-1}} + \frac{1}{x - x_{k+1}} + \dots + \frac{1}{x - x_n}$$

où

$$\left( \frac{y''}{2y'} \right)_{x=x_k} = \frac{1}{x_k - x_1} + \dots + \frac{1}{x_k - x_{k-1}} + \frac{1}{x_k - x_{k+1}} + \dots + \frac{1}{x_k - x_n}$$

on voit donc que les conditions d'équilibre (3) reviennent à ce que l'expression

$$\frac{y''}{2y'} + \frac{B}{A}$$

soit encore  $A y'' + 2 B y'$  s'évanouit pour  $x = x_k$ , ( $k = 1, 2, \dots, n$ ).

Le polynôme  $A y'' + 2 B y'$  du degré  $n + p - 1$  est donc divisible par  $y$  et en désignant le quotient par  $-C$  on a

$$A y'' + 2 B y' + C y = 0.$$

Le polynôme  $y$  du degré  $n$  défini par la relation (4) est donc un de ceux dont l'existence fait l'objet de la proposition de M. Heine.

Il est clair que s'il existait une seconde position d'équilibre, n'importe que cet équilibre fût stable ou non, on en déduirait aussitôt un autre polynôme  $y$  qui satisfait à une équation différentielle telle que (1).

3. Dans ce qui précède nous avons supposé que les points  $X_1, X_2, \dots, X_n$  étaient renfermés dans l'intervalle  $(A_0, A_1)$ . Mais il est clair qu'en se donnant à priori une distribution quelconque de ces points dans les  $p$  intervalles, et en limitant la variabilité de ces points par la condition qu'ils doivent rester toujours dans les intervalles où ils se trouvent d'abord, on peut répéter mot à mot les raisonnements précédents et il existe donc  $(n, p)$  polynômes du degré  $n$  différents qui satisfont à une équation de la forme (1).

CERTAINS POLYNÔMES QUI VÉRIFIENT UNE ÉQUATION DIFFÉRENTIELLE.

polynômes correspondants  $C$  sont aussi différents; en effet on obtient une équation de la forme (1) dont les deux intégrales sont des polynômes  $y_1, y_2$  ce qui est impossible parce qu'on en déduit une relation absurde

$$2 y_1' = \text{Const.} e^{-\int \frac{2B}{A} dx} = \text{Const.} (x - a_0)^{-2a_0} (x - a_1)^{-2a_1} \dots (x - a_p)^{-2a_p}.$$

Pretons maintenant aussi qu'en se donnant la distribution des points  $x_1, x_2, \dots, x_n$  dans les  $p$  intervalles il y a seulement une position d'équilibre et cet équilibre correspondant au maximum du potentiel  $e$ .

En effet d'après les recherches de M. Heine le nombre des polynômes ne peut surpasser  $(n \cdot p)$ .

Considérons maintenant plus particulièrement les fonctions de Lamé dont voici la définition d'après M. Heine.

$$\psi(x) = (x - a_0)(x - a_1) \dots (x - a_p)$$

La fonction de Lamé de l'ordre  $p$  et du degré  $n$  est une fonction du degré  $n$  des quantités

$$A_0 = \sqrt{x - a_0}, A_1 = \sqrt{x - a_1}, \dots, A_p = \sqrt{x - a_p}$$

qui fait à une équation différentielle de la forme

$$\psi(x) \frac{d^2 y}{dx^2} + \frac{1}{2} \psi'(x) \frac{dy}{dx} + \Theta(x) y = 0$$

où  $\psi(x)$  est un polynôme en  $x$  du degré  $p - 1$ .

Les fonctions se distribuent en classes de la manière suivante.

Si  $\psi_1(x)$  est un diviseur quelconque de  $\psi(x)$ , alors on considère comme appartenant à la même classe toutes les fonctions qui sont de la forme

$$\sqrt{\psi_1(x)} V(x)$$

où  $V(x)$  est un polynôme en  $x$ . Naturellement le degré de  $\psi_1(x)$  doit avoir la même parité que  $n$ .

L'équation différentielle à laquelle satisfait le polynôme  $V(x)$  devient

$$\psi(x) \frac{d^2 V}{dx^2} + \left( \frac{1}{2} \psi'(x) + \frac{\psi(x) \psi_1'(x)}{\psi_1(x)} \right) \frac{dV}{dx} + \eta(x) V = 0;$$

41

277

elle est de la forme (1). En supposant réelles et inégales les quantités  $a_0, a_1, \dots, a_p$ , notre proposition devient applicable ; on a en effet

$$\frac{B}{A} = \frac{1}{4} \cdot \frac{\psi'(x)}{\psi(x)} + \frac{1}{2} \cdot \frac{\psi_1'(x)}{\psi_1(x)}$$

en sorte que les nombres  $a_0, a_1, \dots, a_p$  n'ont d'autres valeurs que  $\frac{1}{4}$  et  $\frac{3}{4}$ . Le degré de  $V$  étant  $k$ , les  $(k.p)$  fonctions appartenant à la même classe sont donc réelles, et les racines des diverses équations  $V=0$  se trouvent distribuées de toutes les manières possibles dans les  $p$  intervalles des racines de l'équation  $\psi(x)=0$ .

On doit ce dernier théorème à M. F. Klein (Mathematische Annalen, T. XVIII). La démonstration de M. Klein n'a rien de commun avec les considérations qui précèdent, et ne s'applique pas à notre proposition plus générale.

# XL.

(Paris, C.-R. Acad. Sci., 100, 1885, 439-440)

## Sur quelques théorèmes d'algèbre.

(Note, présentée par M. Hermite.)

$X_n$  le polynôme de Legendre; les racines  $x_1, x_2, \dots, x_n$  de  $X_n = 0$  acquérir un maximum à l'expression

$$(1 - \xi_1^2)(1 - \xi_2^2) \dots (1 - \xi_n^2) \Pi (\xi_k - \xi_l)^2, \quad (k, l = 1, 2, \dots, n)$$

On prend

$$\xi_1 = x_1, \quad \xi_2 = x_2, \quad \dots, \quad \xi_n = x_n.$$

valeur de ce maximum est

$$\frac{2^4 \cdot 3^6 \cdot 4^8 \dots n^{2n}}{3^3 \cdot 5^5 \cdot 7^7 \dots (2n-1)^{2n-1}}.$$

discriminant de  $X_n = 0$ :

$$\Pi (x_k - x_l)^2 = \frac{2^2 \cdot 3^4 \cdot 4^6 \dots n^{2n-2}}{3^1 \cdot 5^3 \cdot 7^5 \dots (2n-1)^{2n-3}}.$$

encore

$$= x^n - 1 \frac{n(n-1)}{1 \cdot 2} x^{n-2} + 1 \cdot 3 \frac{n(n-1)(n-2)(n-3)}{1 \cdot 2 \cdot 3 \cdot 4} x^{n-4} - \dots$$

polynôme défini par la condition

$$\int_{-\infty}^{+\infty} e^{-\frac{1}{2}x^2} U_m U_n dx = 0, \quad (m \geq n);$$

racines  $x_1, x_2, \dots, x_n$  de  $U_n = 0$  font acquérir un maximum à l'expression

$$e^{-\frac{1}{2}(\xi_1^2 + \xi_2^2 + \dots + \xi_n^2)} \Pi (\xi_k - \xi_l)^2,$$

n prenant

$$\xi_1 = x_1, \quad \xi_2 = x_2, \quad \dots, \quad \xi_n = x_n,$$

et la valeur de ce maximum est

$$2^2 \cdot 3^3 \cdot 4^4 \dots n^n e^{-\frac{1}{2}n(n-1)}.$$

Discriminant de  $U_n = 2^2 \cdot 3^3 \cdot 4^4 \dots n^n$ .

Parmi toutes les équations du degré  $n$ , dont les racines sont réelles et ne dépassent pas les limites  $\pm 1$ , celle qui a son discriminant maximum est  $V_n = 0$ , en posant

$$\sqrt{1 - 2xz + z^2} = \sum_0^{\infty} V_n z^n.$$

Discriminant de  $V_n = \frac{1^1 \cdot 2^2 \cdot 3^3 \dots (n-2)^{n-2} \times 2^2 \cdot 3^3 \cdot 4^4 \dots n^n}{1^1 \cdot 3^3 \cdot 5^5 \cdot 7^7 \dots (2n-3)^{2n-3}}$ .

Lorsque  $n$  est très grand, le rapport de ce discriminant à celui de  $K_n$  est sensiblement  $\frac{n\pi}{2}$ .



# XLI.

(Paris, C.-R. Acad. Sci., 100, 1885, 620—622.)

---

## Sur les polynômes de Jacobi.

(Note, présentée par M. Hermite.)

ation

$$\mathcal{F}(-n, n + a + \beta - 1, a, x) = 0$$

mettre sous la forme

$$x^n - \frac{n \cdot a}{1 \cdot c} x^{n-1} + \frac{n(n-1)a(a-1)}{1 \cdot 2 \cdot c(c-1)} x^{n-2} - \dots = 0,$$

$a + n - 1, c = a + \beta + 2n - 2$ . Nous désignerons le premier par  $X$  ou par  $\varphi(n, a, c)$ .  
pour  $x = 0$ ,

$$X = (-1)^n \frac{a(a-1) \dots (a-n+1)}{c(c-1) \dots (c-n+1)},$$

$x = 1$ ,

$$X = \frac{b(b-1) \dots (b-n+1)}{c(c-1) \dots (c-n+1)},$$

nt  $b = \beta + n - 1$ , donc

$$a + b = c.$$

angement de  $x$  en  $1 - x$ , l'équation (1) devient

$$x^n - \frac{n \cdot b}{1 \cdot c} x^{n-1} + \frac{n(n-1)b(b-1)}{1 \cdot 2 \cdot c(c-1)} x^{n-2} - \dots = 0.$$

Soit  $\frac{dX}{dx} = X_1$ , et, en formant la série de Sturm,

$$\begin{aligned} X &= Q X_1 - X_2, \\ X_1 &= Q_1 X_2 - X_3, \\ X_2 &= Q_2 X_3 - X_4, \\ &\dots \end{aligned}$$

oient  $a_1, a_2, a_3, \dots$  les coefficients des plus hautes puissances de  $x$  dans  $X_1, X_2, X_3, \dots$ . On a alors

$$X = \varphi(n, a, c), \quad X_1 = n \varphi(n-1, a, c),$$

ensuite

$$\begin{aligned} a_1^2 X_2 &= n^2(n-1) \frac{a \cdot b}{c^2(c-1)} \varphi(n-2, a-1, c-2), \\ a_1^2 a_2^2 X_3 &= n^3(n-1)^2(n-2) \frac{a^2(a-1)b^2(b-1)}{c^4(c-1)^3(c-2)^2(c-3)} (c-n) \varphi(n-3, a-2, c-4), \\ &\dots \\ \dots, a_{k-1}^2 X_k &= \frac{\prod_0^{k-1} (n-r)^{k-r} (a-r)^{k-1-r} (b-r)^{k-1-r}}{\prod_0^{2k-3} (c-r)^{2k-2-r}} \times \\ &\quad \times \prod_0^{k-3} (c-n-r)^{k-2-r} \varphi(n-k, a-k+1, c-2k+2). \end{aligned}$$

Ces fonctions  $a_1^2 X_2, a_1^2 a_2^2 X_3, \dots$  sont précisément celles qui ont été indiquées par M. Sylvester et qui s'expriment ainsi en fonction des racines  $x_1, x_2, \dots, x_n$  de  $X=0$ :

$$\begin{aligned} &\Sigma (x_1 - x_2)^2 (x - x_3) (x - x_4) \dots, \\ &\Sigma (x_1 - x_2)^2 (x_2 - x_3)^2 (x_3 - x_1)^2 (x - x_4) \dots \end{aligned}$$

On voit par là que les coefficients

$$n^2(n-1) \frac{a b}{c^2(c-1)}, \quad n^3(n-1)^2(n-2) \frac{a^2(a-1)b^2(b-1)}{c^4(c-1)^3(c-2)^2(c-3)} (c-n), \quad \dots,$$

dans les seconds membres de (2), sont égaux aux déterminants

$$\begin{vmatrix} s_0 & s_1 \\ s_1 & s_2 \end{vmatrix}, \quad \begin{vmatrix} s_0 & s_1 & s_2 \\ s_1 & s_2 & s_3 \\ s_2 & s_3 & s_4 \end{vmatrix}, \quad \dots \quad (s_k = x_1^k + x_2^k + \dots + x_n^k).$$

dernière de ces quantités n'est autre chose que le discriminant  $(x_r - x_s)^2$  de l'équation  $X=0$ . On trouve

$$\dots D = \prod_1^n \frac{r^r (a+r-1)^{r-1} (\beta+r-1)^{r-1}}{(a+\beta+n+r-2)^{n+r-2}}.$$

l'équation  $X=0$  ne peut avoir d'autres racines multiples que 0 et 1. On peut assigner sans aucune difficulté le nombre exact des racines positives de  $X=0$ , celui des racines comprises entre 0 et 1, enfin des racines supérieures à 1.

Si  $a > 0$ ,  $\beta > 0$ , les racines sont comprises dans l'intervalle  $(0, 1)$  et l'on peut énoncer la propriété suivante : L'expression

$$\dots \xi_n^\alpha [(1-\xi_1)(1-\xi_2)\dots(1-\xi_n)]^\beta \prod (\xi_r - \xi_s)^2 \quad (r, s = 1, 2, \dots, n)$$

est maximum en posant

$$\xi_1 = x_1, \quad \xi_2 = x_2, \quad \dots, \quad \xi_n = x_n.$$

Il est facile de calculer cette valeur maxima : on trouve

$$\prod_1^n \frac{[r][a+r-1][\beta+r-1]}{[a+\beta+n+r-2]}$$

en remplaçant  $[x]$  au lieu de  $x^x$ .

## XLII.

(Ann. Sci. Éc. norm., Paris, sér. 3, 2, 1885, 93—98.)

---

### Sur une généralisation de la série de Lagrange.

En posant

$$X = x + a \varphi(X),$$

la série de Lagrange donne le développement d'une fonction quelconque de  $X$  sous la forme

$$f(X) = f(x) + \sum_1^{\infty} \frac{a^m}{1 \cdot 2 \dots m} \frac{d^{m-1}}{dx^{m-1}} [f'(x) \varphi^m(x)].$$

En prenant la dérivée par rapport à  $x$ , et écrivant  $f(X)$  au lieu de  $f(x)$ , on a aussi

$$f(X) \frac{dX}{dx} = \sum_0^{\infty} \frac{a^m}{1 \cdot 2 \dots m} \frac{d^m}{dx^m} [f(x) \varphi^m(x)].$$

Sous cette forme, la série de Lagrange est susceptible d'une généralisation élégante, donnée pour la première fois par M. Darboux (Comptes rendus de l'Académie des Sciences, t. LXVIII).

Supposons que les  $r$  variables  $X, Y, Z, \dots$  soient liées aux variables  $x, y, z, \dots$  en même nombre par les  $r$  équations

$$\left. \begin{array}{l} X = x + a \varphi(X, Y, Z, \dots), \\ Y = y + b \psi(X, Y, Z, \dots), \\ Z = z + c \chi(X, Y, Z, \dots), \\ \dots \dots \dots \end{array} \right\} \dots \dots \dots ;$$

$f(X, Y, Z, \dots)$  étant une fonction quelconque, on a le dévelop-

$t$   
 $Z, \dots) \times \Delta$

$$\sum_0^\infty \sum_0^\infty \dots \frac{a^m b^{m'} c^{m''}}{1.2\dots m.1.2\dots m'.1.2\dots m''} \\
\frac{\varphi^{m+m'+m''+\dots}[f(x, y, z, \dots) \varphi^m(x, y, z, \dots) \psi^{m'}(x, y, z, \dots) \chi^{m''}(x, y, z, \dots) \dots]}{d x^m d y^{m'} d z^{m''} \dots},$$

$$\Delta = \begin{vmatrix} \frac{dX}{dx} & \frac{dX}{dy} & \frac{dX}{dz} & \dots \\ \frac{dY}{dx} & \frac{dY}{dy} & \frac{dY}{dz} & \dots \\ \frac{dZ}{dx} & \frac{dZ}{dy} & \frac{dZ}{dz} & \dots \\ \dots & \dots & \dots & \dots \end{vmatrix}.$$

rboux a donné ce développement dans le cas  $r = 2$ .

s la démonstration suivante, je supposerai  $r = 3$ , mais elle s'ap-  
dans le cas général.

me on le verra, le point principal consiste dans l'établissement  
entités

$$\begin{cases} \frac{d}{da} [\Delta f(X, Y, Z)] = \frac{d}{dx} [\Delta f(X, Y, Z) \varphi(X, Y, Z)], \\ \frac{d}{db} [\Delta f(X, Y, Z)] = \frac{d}{dy} [\Delta f(X, Y, Z) \psi(X, Y, Z)], \\ \frac{d}{dc} [\Delta f(X, Y, Z)] = \frac{d}{dz} [\Delta f(X, Y, Z) \chi(X, Y, Z)]. \end{cases}$$

affira, d'ailleurs, de vérifier la première de ces relations, le calcul  
tout à fait analogue pour les deux autres.

s, en développant cette relation, il vient

$$\Delta \left( f'_x \frac{dX}{da} + f'_y \frac{dY}{da} + f'_z \frac{dZ}{da} \right) + f \frac{d\Delta}{da} \\
= \varphi \Delta \left( f'_x \frac{dX}{dx} + f'_y \frac{dY}{dx} + f'_z \frac{dZ}{dx} \right) + f \frac{d(\varphi \Delta)}{dx},$$

sorte qu'il s'agira d'établir les formules

$$\dots \dots \dots \left\{ \begin{array}{l} \frac{dX}{da} = \varphi \frac{dX}{dx}, \\ \frac{dY}{da} = \varphi \frac{dY}{dx}, \\ \frac{dZ}{da} = \varphi \frac{dZ}{dx} \end{array} \right.$$

$$\dots \dots \dots \frac{d\Delta}{da} = \frac{d(\varphi \Delta)}{dx}.$$

La différentiation de la première des formules (1) donne

$$\dots \dots \dots \left\{ \begin{array}{l} (1 - a \varphi'_x) \frac{dX}{da} = \varphi + a \varphi'_y \frac{dY}{da} + a \varphi'_z \frac{dZ}{da}, \\ (1 - a \varphi'_x) \frac{dX}{dx} = 1 + a \varphi'_y \frac{dY}{dx} + a \varphi'_z \frac{dZ}{dx}, \end{array} \right.$$

l'on obtient de même

$$\dots \dots \dots \left\{ \begin{array}{l} b \psi'_x \frac{dX}{da} + (b \psi'_y - 1) \frac{dY}{da} + b \psi'_z \frac{dZ}{da} = 0, \\ c \chi'_x \frac{dX}{da} + c \chi'_y \frac{dY}{da} + (c \chi'_z - 1) \frac{dZ}{da} = 0, \end{array} \right.$$

$$\dots \dots \dots \left\{ \begin{array}{l} b \psi'_x \frac{dX}{dx} + (b \psi'_y - 1) \frac{dY}{dx} + b \psi'_z \frac{dZ}{dx} = 0, \\ c \chi'_x \frac{dX}{dx} + c \chi'_y \frac{dY}{dx} + (c \chi'_z - 1) \frac{dZ}{dx} = 0. \end{array} \right.$$

Les équations (6) déterminent les rapports  $\frac{dX}{da} : \frac{dY}{da} : \frac{dZ}{da}$ , les

équations (7) les rapports  $\frac{dX}{dx} : \frac{dY}{dx} : \frac{dZ}{dx}$ . Or, les coefficients dans

les systèmes (6) et (7) étant les mêmes, on a

$$\frac{dX}{da} : \frac{dY}{da} : \frac{dZ}{da} = \frac{dX}{dx} : \frac{dY}{dx} : \frac{dZ}{dx}.$$

Dès lors les équations (5) mettent en évidence les relations (3).

e à vérifier la formule (4). On a

$$\begin{aligned} \Delta_1 &= \begin{vmatrix} \frac{d^2 X}{dx da} & \frac{dX}{dy} & \frac{dX}{dz} \\ \frac{d^2 Y}{dx da} & \frac{dY}{dy} & \frac{dY}{dz} \\ \frac{d^2 Z}{dx da} & \frac{dZ}{dy} & \frac{dZ}{dz} \end{vmatrix} + \Delta_2 + \Delta_3. \\ \Delta_2 &= \begin{vmatrix} \frac{dX}{dx} & \frac{d^2 X}{dy da} & \frac{dX}{dz} \\ \frac{dY}{dx} & \frac{d^2 Y}{dy da} & \frac{dY}{dz} \\ \frac{dZ}{dx} & \frac{d^2 Z}{dy da} & \frac{dZ}{dz} \end{vmatrix} + \begin{vmatrix} \frac{dX}{dx} & \frac{dX}{dy} & \frac{d^2 X}{dz da} \\ \frac{dY}{dx} & \frac{dY}{dy} & \frac{d^2 Y}{dz da} \\ \frac{dZ}{dx} & \frac{dZ}{dy} & \frac{d^2 Z}{dz da} \end{vmatrix} \end{aligned}$$

t à  $\Delta_1$ , on a, à cause des relations (3),

$$\Delta_1 = \begin{vmatrix} \frac{d}{dx} \left( \varphi \frac{dX}{dx} \right) & \frac{dX}{dy} & \frac{dX}{dz} \\ \frac{d}{dx} \left( \varphi \frac{dY}{dx} \right) & \frac{dY}{dy} & \frac{dY}{dz} \\ \frac{d}{dx} \left( \varphi \frac{dZ}{dx} \right) & \frac{dZ}{dy} & \frac{dZ}{dz} \end{vmatrix}.$$

nt ensuite

$$\Delta_2 = \begin{vmatrix} \frac{dX}{dx} & \frac{d}{dy} \left( \varphi \frac{dX}{dx} \right) & \frac{dX}{dz} \\ \frac{dY}{dx} & \frac{d}{dy} \left( \varphi \frac{dY}{dx} \right) & \frac{dY}{dz} \\ \frac{dZ}{dx} & \frac{d}{dy} \left( \varphi \frac{dZ}{dx} \right) & \frac{dZ}{dz} \end{vmatrix} = \begin{vmatrix} \frac{dX}{dx} & \varphi \frac{d^2 X}{dy dx} & \frac{dX}{dz} \\ \frac{dY}{dx} & \varphi \frac{d^2 Y}{dy dx} & \frac{dY}{dz} \\ \frac{dZ}{dx} & \varphi \frac{d^2 Z}{dy dx} & \frac{dZ}{dz} \end{vmatrix}$$

$$\Delta_2 = \begin{vmatrix} \varphi \frac{dX}{dx} & \frac{d^2 X}{dy dx} & \frac{dX}{dz} \\ \varphi \frac{dY}{dx} & \frac{d^2 Y}{dy dx} & \frac{dY}{dz} \\ \varphi \frac{dZ}{dx} & \frac{d^2 Z}{dy dx} & \frac{dZ}{dz} \end{vmatrix},$$

ême

$$\Delta_3 = \begin{vmatrix} \varphi \frac{dX}{dx} & \frac{dX}{dy} & \frac{d^2 X}{dz dx} \\ \varphi \frac{dY}{dx} & \frac{dY}{dy} & \frac{d^2 Y}{dz dx} \\ \varphi \frac{dZ}{dx} & \frac{dZ}{dy} & \frac{d^2 Z}{dz dx} \end{vmatrix}.$$

Les équations (8), (9) et (10) donnent de suite

$$\Delta_1 + \Delta_2 + \Delta_3 = \frac{d \Delta}{d a} = \frac{d (\varphi \Delta)}{d x},$$

est-à-dire la formule (4).

La première des équations (2) est ainsi établie parfaitement, les deux autres s'obtiennent de la même manière.

Par une application répétée de ces relations, on trouve de suite

$$1) . \left\{ \begin{aligned} & \frac{d^{m+m'+m''} [\Delta f(X, Y, Z)]}{d a^m d b^{m'} d c^{m''}} \\ &= \frac{d^{m+m'+m''} [\Delta f(X, Y, Z) \varphi^m(X, Y, Z) \psi^{m'}(X, Y, Z) \chi^{m''}(X, Y, Z)]}{d x^m d y^{m'} d z^{m''}}. \end{aligned} \right.$$

Pour avoir le coefficient de  $\frac{a^m b^{m'} c^{m''}}{1.2 \dots m.1.2 \dots m'.1.2 \dots m''}$  dans le développement de  $\Delta f(X, Y, Z)$ , il suffit de supposer  $a = b = c = 0$ , dans cette formule (11). Or, dans cette supposition, il vient

$$\begin{aligned} \frac{d X}{d x} &= 1, & \frac{d X}{d y} &= 0, & \frac{d X}{d z} &= 0, \\ \frac{d Y}{d x} &= 0, & \frac{d Y}{d y} &= 1, & \frac{d Y}{d z} &= 0, \\ \frac{d Z}{d x} &= 0, & \frac{d Z}{d y} &= 0, & \frac{d Z}{d z} &= 1, \end{aligned}$$

donc  $\Delta = 1$ ; de plus  $X = x$ ,  $Y = y$ ,  $Z = z$ , en sorte que ce coefficient est égal à

$$\frac{d^{m+m'+m''} [f(x, y, z) \varphi^m(x, y, z) \psi^{m'}(x, y, z) \chi^{m''}(x, y, z)]}{d x^m d y^{m'} d z^{m''}},$$

comme nous l'avons annoncé.

Je terminerai par la remarque suivante. Dans le Tome 54 du Journal Crèlle, M. Heine a déduit la formule de Lagrange à l'aide du calcul des variations. Cette démonstration peut être généralisée facilement, de manière à obtenir la formule que nous venons de démontrer, le



inant fonctionnel  $\Delta$  s'introduisant alors de la manière la plus  
elle. Mais les formules (2) et la formule (11) qui s'en déduit  
liatement paraissent assez remarquables en elles-mêmes : c'est ce  
ous a fait préférer la méthode plus élémentaire que nous venons  
velopper.

---

# XLIII.

(Bull. Sci. math., Paris, sér. 2, 9, 1885, 306—311.)

Sur l'intégrale  $\int_0^\infty \frac{e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}}.$

1. Nous nous proposons d'obtenir le développement de cette intégrale suivant les puissances descendantes de  $a$ , développement qui peut servir utilement pour le calcul numérique dans le cas où le nombre positif  $a$  est très grand et que  $b$  ne l'est pas.

La méthode qui se présente d'abord pour cet objet est la suivante.

$$P = 1 : \left(1 + \frac{x}{a}\right)^{a+b},$$

ors

$$\log P = -(a+b) \left( \frac{x}{a} - \frac{x^2}{2a^2} + \frac{x^3}{3a^3} - \dots \right)$$

a bien

$$\log P = -x + \frac{A_1}{a} + \frac{A_2}{a^2} + \frac{A_3}{a^3} + \dots,$$

$$A_1 = \frac{1}{2} x^2 - b x,$$

$$A_2 = \frac{1}{8} x^3 + \frac{1}{2} b x^2,$$

$$A_3 = \frac{1}{4} x^4 - \frac{1}{3} b x^3,$$

$$\dots \dots \dots$$

Il s'ensuit

$$P = e^{-x} \times e^{\frac{A_1}{a} + \frac{A_2}{a^2} + \frac{A_3}{a^3} + \dots},$$

$$P = e^{-x} \left( 1 + \frac{B_1}{a} + \frac{B_2}{a^2} + \frac{B_3}{a^3} + \dots \right),$$

sant

$$B_1 = A_1,$$

$$B_2 = A_2 + \frac{1}{2} A_1^2,$$

$$B_3 = A_3 + A_1 A_2 + \frac{1}{6} A_1^3,$$

$$\dots$$

l'intégrale proposée se met maintenant sous la forme

$$\int_0^\infty \left( 1 + \frac{B_1}{a} + \frac{B_2}{a^2} + \frac{B_3}{a^3} + \dots \right) e^{-2x} dx,$$

il ne reste plus qu'à effectuer les intégrations à l'aide de la formule

$$\int_0^\infty x^k e^{-2x} dx = \frac{\Gamma(k)}{2^{k+1}}.$$

On obtient ainsi, pour les premiers termes,

$$\frac{1}{2} + \frac{-2b+1}{8a} + \frac{4b^2-2b-1}{32a^2} + \frac{-8b^3+10b-1}{128a^3} + \dots$$

On voit, comme on le voit, cette méthode ne donne aucune lumière sur la question de savoir s'il faut ajouter à un nombre fini de termes du développement pour obtenir la valeur exacte de l'intégrale et, de plus, elle devient très pénible si l'on voulait pousser plus loin des calculs.

Nous allons développer maintenant une autre méthode qui ne présente pas ces défauts.

On trouve, par la différentiation,

$$\frac{x^k e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b}} = -\frac{x^k e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b}} + \frac{k x^{k-1} e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b}} - \frac{a+b}{a} \frac{x^k e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b+1}},$$

on peut mettre sous la forme

$$\frac{x^k e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b}} = -\frac{2 x^k e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b}} + \frac{k x^{k-1} e^{-x}}{\left(1 + \frac{x}{a}\right)^{a+b}} + \frac{x^k (x-b) e^{-x}}{a \left(1 + \frac{x}{a}\right)^{a+b+1}}.$$

On en conclut, lorsque  $k > 0$ ,

$$\int_0^\infty \frac{x^k e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = \frac{k}{2} \int_0^\infty \frac{x^{k-1} e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} + \frac{1}{2a} \int_0^\infty \frac{x^k (x-b) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+1}},$$

pour  $k=0$

$$\dots \int_0^{\infty} \frac{e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = \frac{1}{2} + \frac{1}{2a} \int_0^{\infty} \frac{(x-b) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+1}}.$$

En écrivant dans la formule (1) successivement  $k-1, k-2, \dots$  au lieu de  $k$ , on trouvera par une combinaison bien facile de ces équations et la formule (2)

$$\int_0^{\infty} \frac{x^k e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = \frac{\Pi(k)}{2^{k+1}} + \frac{1}{2a} \int_0^{\infty} \frac{(x-b) T_k(x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+1}},$$

$$T_k(x) = x^k + \frac{k}{2} x^{k-1} + \frac{k(k-1)}{2 \cdot 2} x^{k-2} + \frac{k(k-1)(k-2)}{2 \cdot 2 \cdot 2} x^{k-3} + \dots$$

Il importe de remarquer que la valeur de  $T_k(x)$  pour  $x=0$  est  $k! : 2^k$ , en sorte qu'on peut écrire

$$\int_0^{\infty} \frac{x^k e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = \frac{1}{2} T_k(0) + \frac{1}{2a} \int_0^{\infty} \frac{(x-b) T_k(x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+1}}.$$

Soit maintenant  $f(x)$  un polynôme quelconque de  $x$ , on aura évidemment

$$\int_0^{\infty} \frac{f(x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = \frac{1}{2} \overline{f(0)} + \frac{1}{2a} \int_0^{\infty} \frac{(x-b) \overline{f(x)} e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+1}},$$

désignant symboliquement par  $\overline{f(x)}$  le polynôme obtenu en remplaçant les diverses puissances  $x, x^2, x^3, \dots$  dans  $f(x)$  par  $T_1(x), T_2(x), T_3(x), \dots$

En écrivant  $b+n$  au lieu de  $b$ , nous avons

$$\int_0^{\infty} \frac{f(x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n}} = \frac{1}{2} \overline{f(0)} + \frac{1}{2a} \int_0^{\infty} \frac{(x-b-n) \overline{f(x)} e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n+1}}$$

Nous allons appliquer cette formule dans le cas particulier  $f(x) = (b-x)^k$ ; alors il viendra

$$\begin{aligned} \overline{f(x)} &= b^k - \frac{k}{1} b^{k-1} (x + \frac{1}{2}) + \frac{k(k-1)}{1 \cdot 2} b^{k-2} (x^2 + x + \frac{1}{2}) - \\ &\quad - \frac{k(k-1)(k-2)}{1 \cdot 2 \cdot 3} b^{k-3} (x^3 + \frac{3}{2} x^2 + \frac{3}{2} x + \frac{3}{4}) + \dots \end{aligned}$$

en

$$f(x) = (b-x)^k - \frac{k}{2} (b-x)^{k-1} + \frac{k(k-1)}{2 \cdot 2} (b-x)^{k-2} - \dots$$

posant donc

$$U_k(b) = b^k - \frac{k}{2} b^{k-1} + \frac{k(k-1)}{2 \cdot 2} b^{k-2} - \dots,$$

at

$$\frac{(b-x)^k e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n}} = \frac{1}{2} U_k(b) + \frac{1}{2a} \int_0^\infty \frac{(x-b-n) U_k(b-x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n+1}}.$$

là il suit immédiatement qu'en supposant

$$V(b) = c_0 + c_1 b + c_2 b^2 + \dots + c_k b^k,$$

ra

$$\frac{V(b-x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n}} = \frac{1}{2} [V(b)] + \frac{1}{2a} \int_0^\infty \frac{(x-b-n) [V(b-x)] e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n+1}},$$

signant par  $[V(b)]$  le polynôme obtenu en remplaçant dans  $b$  par  $U_1(b)$ ,  $b^2$  par  $U_2(b)$ ,  $b^3$  par  $U_3(b)$ , ..., tandis que naturellement,  $[V(b-x)]$  s'obtient en écrivant  $b-x$  au lieu de  $b$  dans  $[V(b)]$ . qui précède suppose, bien entendu, que les coefficients  $c_0, c_1, c_2, \dots$  convergent point  $b$ . Si cela avait lieu, il faudrait d'abord écrire  $B$  au lieu de  $b$  dans ces coefficients, opérer ensuite comme il vient d'être dit et rétablir enfin de nouveau  $b$  au lieu de  $B$ . Ainsi la valeur de  $[V(b-x)]$  dans le premier membre de (4) est égale à

$$c_0 + c_1 (b-x) + c_2 (b-x)^2 + \dots + c_k (b-x)^k,$$

il ne faut pas substituer  $b-x$  à la place de  $b$  dans les coefficients  $c_1, \dots, c_k$ .

Revenons maintenant à la formule (2), que nous écrivons ainsi

$$\int_0^\infty \frac{e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = V_0(b) + \frac{R_1}{a},$$

en posant

$$V_0(b) = \frac{1}{2}, \quad R_1 = \int_0^\infty \frac{(x-b) V_0(b-x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+1}}.$$

Quant à l'expression  $R_1$ , nous pouvons la transformer à l'aide de la formule (4), où il faut prendre  $V(b) = -b V_0(b)$ ,  $n=1$ . Il vient

$$R_1 = V_1(b) + \frac{R_2}{a},$$

en posant

$$V_1(b) = -\frac{1}{2}[b V_0(b)], \quad R_2 = \int_0^\infty \frac{(x-b-1) V_1(b-x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+2}}.$$

Cette expression  $R_2$  peut, de nouveau, se transformer à l'aide de (4) en prenant  $V(b) = -(b+1) V_1(b)$  et  $n=2$ . Il vient

$$R_2 = V_2(b) + \frac{R_3}{a},$$

en posant

$$V_2(b) = -\frac{1}{2}[(b+1) V_1(b)], \quad R_3 = \int_0^\infty \frac{(x-b-2) V_2(b-x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+3}}.$$

Il est évident qu'on peut continuer ainsi et l'on trouve le résultat suivant:

$$\int_0^\infty \frac{e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b}} = V_0(b) + \frac{V_1(b)}{a} + \frac{V_2(b)}{a^2} + \dots + \frac{V_{n-1}(b)}{a^{n-1}} + \frac{R_n}{a^n}.$$

Ici les polynômes  $V_0(b)$ ,  $V_1(b)$ ,  $V_2(b)$ , ... se calculent de proche en proche par les relations

$$\begin{aligned} V_0(b) &= \frac{1}{2}, \\ V_1(b) &= -\frac{1}{2}[b V_0(b)], \\ V_2(b) &= -\frac{1}{2}[(b+1) V_1(b)], \\ V_3(b) &= -\frac{1}{2}[(b+2) V_2(b)], \\ V_4(b) &= -\frac{1}{2}[(b+3) V_3(b)], \\ &\dots \end{aligned}$$

as rappelons que  $[f(b)]$  s'obtient en ordonnant  $f(b)$  suivant les puissances de  $b$  et en remplaçant alors  $b^k$  par

$$b^k = \frac{k}{2} b^{k-1} + \frac{k(k-1)}{2 \cdot 2} b^{k-2} - \frac{k(k-1)(k-2)}{2 \cdot 2 \cdot 2} b^{k-3} + \dots$$

uite le reste  $R_n : a^n$  s'exprime à l'aide du polynôme  $V_{n-1}(b)$  ainsi :

$$R_n : a^n = \int_0^\infty \frac{(x-b-n+1) V_{n-1}(b-x) e^{-x} dx}{\left(1 + \frac{x}{a}\right)^{a+b+n}} : a^n.$$

peut remarquer que  $V_n(b)$  est la valeur de  $R_n$  pour  $a = \infty$  : donc

$$V_n(b) = \int_0^\infty (x-b-n+1) V_{n-1}(b-x) e^{-2x} dx ;$$

ela revient, comme il est facile de le voir, à l'expression

$$V_n(b) = -\frac{1}{2} [(b+n-1) V_{n-1}(b)].$$

trouve sans difficulté :

$$\begin{aligned} &= +\frac{1}{2}, \\ &= -\frac{1}{4}b + \frac{1}{8}, \\ &= +\frac{1}{8}b^2 - \frac{1}{16}b - \frac{1}{32}, \\ &= -\frac{1}{16}b^3 + \frac{5}{64}b - \frac{1}{128}, \\ &= +\frac{1}{32}b^4 - \frac{1}{32}b^3 - \frac{11}{128}b^2 - \frac{7}{256}b + \frac{1}{512}, \\ &= -\frac{1}{64}b^5 - \frac{1}{128}b^4 + \frac{31}{256}b^3 + \frac{1}{256}b^2 + \frac{39}{1024}b - \frac{143}{2048}, \\ &= +\frac{1}{128}b^6 + \frac{31}{1024}b^5 - \frac{239}{2048}b^4 - \frac{73}{1024}b^3 + \frac{5}{64}b^2 - \frac{567}{4096}b + \frac{1997}{8192}. \\ &\dots \dots \dots \end{aligned}$$

Le premier calcul se trouve vérifié ainsi ; nous avons obtenu de ce reste de la série sous forme finie.

---

## XLIV.

(Paris, C.-R. Acad. Sci., 101, 1885, 153—154.)

### Sur une fonction uniforme.

(Note présentée par M. Hermite.)

Le caractère analytique de la fonction  $\zeta(z)$ , qui est définie pour les valeurs de  $z$  dont la partie réelle surpasse l'unité par la série

$$1 + \frac{1}{2^z} + \frac{1}{3^z} + \frac{1}{4^z} + \dots,$$

été complètement dévoilé par Riemann qui a montré que

$$\zeta(z) = \frac{1}{z-1}$$

est holomorphe dans tout le plan.

Les zéros de la fonction  $\zeta(z)$  sont d'abord

$$-2, -4, -6, -8, \dots;$$

et en a, en outre, une infinité d'autres, qui sont tous imaginaires, la partie réelle restant comprise entre 0 et 1.

Riemann a annoncé comme très probable que toutes ces racines imaginaires sont de la forme  $\frac{1}{2} + ai$ ,  $a$  étant réel.

Je suis parvenu à mettre cette proposition hors de doute par une démonstration rigoureuse. Je vais indiquer la voie qui m'a conduit à ce résultat.

D'après une remarque due à Euler,

$$1 : \zeta(z) = \prod \left(1 - \frac{1}{p^z}\right),$$

représentant tous les nombres premiers, ou encore

$$1 : \zeta(z) = 1 - \frac{1}{2^z} - \frac{1}{3^z} - \frac{1}{5^z} + \frac{1}{6^z} - \frac{1}{7^z} + \frac{1}{10^z} - \dots$$



étude plus approfondie de la série qui figure ici dans le second qui conduit au but désiré. On peut démontrer, en effet, que la série est convergente et définit une fonction analytique tant que la partie réelle de  $z$  surpasse  $\frac{1}{2}$ .

Il est évident, d'après cela, que  $\zeta(z)$  ne s'évanouit pour aucune valeur de  $z$  dont la partie réelle surpasse  $\frac{1}{2}$ . Mais l'équation  $\zeta(z) = 0$  ne peut admettre non plus des racines imaginaires dont la partie réelle est égale à  $\frac{1}{2}$ . En effet, en admettant l'existence d'une telle racine  $z = z_1$ , on a aussi  $\zeta(1 - z_1) = 0$ , comme le montre la relation entre  $\zeta(z)$  et  $\zeta(1 - z)$  établie par Riemann. Or, la partie réelle de  $1 - z_1$  est supérieure à  $\frac{1}{2}$ .

Par conséquent, toutes les racines imaginaires de  $\zeta(z) = 0$  sont de la forme  $\frac{1}{2} + ai$ ,  $a$  étant réel.

# XLV.

(Paris, C.-R. Acad. Sci., 101, 1885, 368—370).

Sur une loi asymptotique dans la théorie des nombres.

(Note présentée par M. Hermite.)

Le théorème énoncé dans les Comptes rendus, p. 153, que la série

$$1 - \frac{1}{2^s} - \frac{1}{3^s} - \frac{1}{5^s} + \frac{1}{6^s} - \dots,$$

tendue par le développement du produit infini  $\prod \left(1 - \frac{1}{p^s}\right)$ , est convergente pour  $s > \frac{1}{2}$ , conduit à une conséquence importante relative à la fonction de M. Tchebychef  $\theta(x) =$  somme des logarithmes des nombres premiers qui ne surpassent pas  $x$ .

En désignant par  $f(n)$  le nombre des diviseurs de  $n$ , je rappelle ce résultat dû à Dirichlet, que

$$\frac{f(1) + f(2) + \dots + f(n) - n \log n + (2C - 1)n}{\sqrt{n}}$$

est comprise entre deux limites finies,  $C$  étant la constante eulérienne.

On en conclut facilement que la série

$$\sum_1^\infty \frac{f(n) - \log n - 2C}{n^s}$$

est convergente pour  $s > \frac{1}{2}$ .

Voici maintenant deux théorèmes relatifs aux séries de la forme

$\sum \frac{\lambda'(n)}{n^s}$  qui nous sont nécessaires :

théorème I. — Lorsque la série  $\sum_1^{\infty} \frac{\lambda(n)}{n^s}$ , où  $s > 0$ , est convergente,

$$\lim_{n \rightarrow \infty} \frac{\lambda(1) + \lambda(2) + \dots + \lambda(n)}{n^s} = 0 \quad (n = \infty).$$

théorème II. — Lorsque les deux séries

$$\sum_1^{\infty} \frac{\lambda(n)}{n^s} \quad \text{et} \quad \sum_1^{\infty} \frac{\mu(n)}{n^s}$$

sont convergentes pour  $s = \alpha > 0$  et que les séries

$$\sum_1^{\infty} \frac{|\lambda(n)|}{n^s}, \quad \sum_1^{\infty} \frac{|\mu(n)|}{n^s}$$

sont convergentes pour  $s = \alpha + \beta$ , alors la série obtenue en multipliant les deux premières

$$\sum_1^{\infty} \frac{\nu(n)}{n^s},$$

$$\nu(n) = \sum \lambda(d) \mu\left(\frac{n}{d}\right),$$

présentant tous les diviseurs de  $n$ , est convergente pour  $s = \alpha + \frac{1}{2}\beta$ .  
 En remplaçant, dans les séries (A) et (B), chaque terme par sa valeur absolue, les nouvelles séries convergent pour  $s > 1$ . En multipliant les séries (A) et (B), la série obtenue sera convergente pour  $s > \frac{3}{4}$ , d'après le théorème II.

On obtient ainsi

$$\sum_1^{\infty} \frac{1 - g(n)}{n^s},$$

$$g(1) = 2C,$$

où  $p$  est premier,  $g(p^k) = \log p$ , tandis que  $g(n) = 0$  lorsque  $n$  n'est pas de la forme  $p^k$ . On en conclut, d'après le théorème I,

$$\lim_{n \rightarrow \infty} \frac{n - g(1) - g(2) - \dots - g(n)}{n^s} = 0 \quad (n = \infty, \quad s > \frac{3}{4});$$

mais on voit facilement que

$$g(1) + g(2) + \dots + g(n) = 2C + \Theta(n) + \Theta\left(n^{\frac{1}{2}}\right) + \Theta\left(n^{\frac{1}{3}}\right) + \dots$$

en sorte que, en posant

$$\Theta(n) + \Theta\left(n^{\frac{1}{2}}\right) + \Theta\left(n^{\frac{1}{3}}\right) + \dots = n + A_n n^s.$$

on trouve

$$\lim A_n = 0 \quad \text{pour } n = \infty.$$

Il est facile d'en déduire qu'on a aussi

$$\Theta(n) = n + B_n n^s,$$

où

$$\lim B_n = 0$$

dès que  $s > \frac{3}{4}$ .

Ce résultat conduit à cette conséquence que, quelque petit que soit un nombre positif  $h$ , le nombre des nombres premiers compris entre

$$n \quad \text{et} \quad (1+h)n$$

finir toujours par croître au delà de toute limite, quand  $n$  croît indéfiniment.

---

## XLVI.

Amsterdam, Versl. K. Akad. Wet., Afd. Nat., sér. 3, 2, 1886, 101—104)

---

r quelques formules qui se rapportent à la théorie des  
fonctions elliptiques.

as les formules qui suivent on doit toujours, sauf indication con-  
, attribuer au nombre  $n$  placé sous le signe  $\Sigma$  les valeurs entières  
itives

$$n = 1, 2, 3, 4, \dots$$

mbre  $m$  désignera les nombres impairs

$$m = 1, 3, 5, 7, \dots$$

suite  $D$  représente un nombre entier positif ou négatif, mais je  
se toujours que  $D$  n'est divisible par aucun carré hors l'unité.  
listingue quatre cas.

I.

$D > 0$ ,  $D \equiv 2, 3 \pmod{4}$ . En posant

$$\dots \dots \dots F(x) = \sum \left( \frac{D}{m} \right) e^{-\frac{m^2 \pi x}{4D}}$$

fonction jouit de ces propriétés :

$$\dots \dots \dots F\left(\frac{1}{x}\right) = \sqrt{x} F(x),$$

$$\dots \dots \dots F(x + Di) = e^{-\frac{\pi i}{4}} F(x),$$

est le symbole de Legendre, généralisé par Jacobi, avec la con-

n ordinaire que  $\left(\frac{D}{m}\right) = 0$ , lorsque  $D$  et  $m$  ne sont pas premiers

tre eux. J'ajoute que, dans ce qui suit, on suppose encore  $\left(\frac{r}{n}\right) = \left(\frac{r}{-n}\right)$ .  
 voir p. e. Kronecker, Berliner Monatsberichte, Juni 1876).

## II.

$D < 0$ ,  $D \equiv 2, 3 \pmod{4}$ . En posant

$$\dots \dots \dots G(x) = \sum \left(\frac{D}{m}\right) m e^{\frac{m^2 \pi x}{4D}}$$

aura

$$\dots \dots \dots G\left(\frac{1}{x}\right) = (\sqrt{x})^3 G(x),$$

$$\dots \dots \dots G(x - D i) = e^{-\frac{\pi i}{4}} G(x).$$

## III.

$D > 0$ ,  $D \equiv 1 \pmod{4}$ . En posant

$$\dots \dots \dots \begin{cases} F_1(x) = \sum \left(\frac{n}{D}\right) e^{-\frac{n^2 \pi x}{D}}, \\ F_2(x) = \sum (-1)^n \left(\frac{n}{D}\right) e^{-\frac{n^2 \pi x}{D}}, \\ F_3(x) = \sum \left(\frac{m}{D}\right) e^{-\frac{m^2 \pi x}{4D}}, \end{cases}$$

aura

$$\dots \dots \dots \begin{cases} F_1\left(\frac{1}{x}\right) = \sqrt{x} F_1(x), \\ F_2\left(\frac{1}{x}\right) = (-1)^{\frac{D-1}{4}} \sqrt{x} F_3(x), \\ F_3\left(\frac{1}{x}\right) = (-1)^{\frac{D-1}{4}} \sqrt{x} F_2(x), \end{cases}$$

$$\dots \dots \dots \begin{cases} F_1(x + D i) = F_2(x), \\ F_2(x + D i) = F_1(x), \\ F_3(x + D i) = e^{-\frac{\pi i}{4}} F_3(x). \end{cases}$$

fois, ces formules sont en défaut dans le cas  $D = 1$ , mais en dans ce cas au lieu de  $(\gamma)$

$$\begin{aligned} F_1(x) &= \sum_{-\infty}^{+\infty} e^{-n^2 \pi x}, \\ F_2(x) &= \sum_{-\infty}^{+\infty} (-1)^n e^{-n^2 \pi x}, \\ F_3(x) &= \sum_{-\infty}^{+\infty} e^{-\frac{(2n-1)^2 \pi x}{4}}, \end{aligned}$$

ions  $(\gamma')$  et  $(\gamma'')$  restent vraies.

#### IV

,  $D \equiv 1 \pmod{4}$ . En posant

$$\left\{ \begin{aligned} G_1(x) &= \sum \left( \frac{n}{D} \right) n e^{\frac{n^2 \pi x}{D}}, \\ G_2(x) &= \sum (-1)^n \left( \frac{n}{D} \right) n e^{\frac{n^2 \pi x}{D}}, \\ 2 G_3(x) &= \sum \left( \frac{m}{D} \right) m e^{\frac{m^2 \pi x}{D}}, \end{aligned} \right.$$

$$\left\{ \begin{aligned} G_1\left(\frac{1}{x}\right) &= (\sqrt{x})^3 G_1(x), \\ G_2\left(\frac{1}{x}\right) &= (-1)^{\frac{D-1}{4}} (\sqrt{x})^3 G_3(x), \\ G_3\left(\frac{1}{x}\right) &= (-1)^{\frac{D-1}{4}} (\sqrt{x})^3 G_2(x), \end{aligned} \right.$$

$$\left\{ \begin{aligned} G_1(x - D i) &= G_2(x), \\ G_2(x - D i) &= G_1(x), \\ G_3(x - D i) &= e^{-\frac{\pi i}{4}} G_3(x). \end{aligned} \right.$$

out on doit supposer positive la partie réelle de  $x$  et de  $\sqrt{x}$ .

On voit bien les conséquences qui se rattachent à ces formules et  
r lesquelles j'aurai peut-être l'occasion de revenir plus tard.

Pour le moment je me borne à cette indication que toutes ces for-  
mules se déduisent sans peine à l'aide des propriétés fondamentales de  
fonction  $\theta$  d'une part et d'autre part des formules que Gauss a  
onnées dans son célèbre mémoire intitulé: *Summatio quarumdam se-  
erum singularium*, 1808. Oeuvres, tome II.

---



## XLVII.

dam, Versl. K. Akad. Wet., Afd. Nat., sér. 3, 2, 1886, 210—216.)

---

### Sur quelques intégrales définies.

dre dans les Exercices de calcul intégral (t. II, p. 189) a donné de l'intégrale

$$\int_0^{\infty} \frac{\sin mx}{e^{\frac{1}{2}\pi x} - 1} dx = \frac{1}{4} \frac{e^m + 1}{e^m - 1} - \frac{1}{2m}$$

sur laquelle Abel est revenu plus d'une fois (Oeuvres, tome I, Édition de Sylow et Lie).

e du mémoire de Riemann: „Ueber die Anzahl der Prim-  
unter einer gegebenen Grenze" m'a conduit à cette remarque  
ait regarder la formule de Legendre comme le cas le plus  
e toute une série de formules qui présentent un caractère  
ment arithmétique.

ce qui suit je me bornerai à donner deux exemples qui feront  
e suffisamment le caractère des formules nouvelles, sans en  
présenter dès à présent, le système complet.

un nombre entier positif impair ( $p > 1$ ) sans diviseur carré

$$f(x) = \sum_1^{p-1} \left( \frac{n}{p} \right) x^n$$

le  $\left( \frac{n}{p} \right)$  étant pris dans le même sens que dans ma communi-  
Septembre 1885 (pag. 101 de ce volume).

Cela posé, on a lorsque

$$p \equiv 1 \pmod{4}$$

$$A) \quad \dots \quad \int_0^{\infty} \frac{f(e^{-x})}{1 - e^{-px}} \sin\left(\frac{p t x}{2 \pi}\right) dx = \frac{\pi}{V p} \cdot \frac{f(e^{-t})}{1 - e^{-pt}}.$$

En supposant au contraire

$$p \equiv 3 \pmod{4}$$

on a

$$B) \quad \dots \quad \int_0^{\infty} \frac{f(e^{-x})}{1 - e^{-px}} \cos\left(\frac{p t x}{2 \pi}\right) dx = \frac{\pi}{V p} \cdot \frac{f(e^{-t})}{1 - e^{-pt}}.$$

Dans ces formules (A) et (B) la racine  $V p$  doit être prise positivement, et cette détermination du signe correspond précisément à celle que Gauss a donnée dans le mémoire *Summatio etc*, Oeuvres, tome II

C'est par le développement en série de l'expression

$$\frac{f(e^{-x})}{1 - e^{-px}}$$

que j'ai obtenu ces résultats

En posant pour abrégé

$$\varphi(s) = \sum_1^{\infty} \left(\frac{n}{p}\right) \frac{1}{n^s}$$

on obtiens

$$C) \quad \dots \quad \frac{f(e^{-x})}{1 - e^{-px}} = \frac{V p}{\pi} \left\{ \varphi(2) \frac{p x}{2 \pi} - \varphi(4) \frac{p^3 x^3}{2^3 \pi^3} + \varphi(6) \frac{p^5 x^5}{2^5 \pi^5} - \dots \right\}$$

lorsque  $p \equiv 1 \pmod{4}$ ,

$$D) \quad \dots \quad \frac{f(e^{-x})}{1 - e^{-px}} = \frac{V p}{\pi} \left\{ \varphi(1) - \varphi(3) \frac{p^2 x^2}{2^2 \pi^2} + \varphi(5) \frac{p^4 x^4}{2^4 \pi^4} - \dots \right\}$$

lorsque  $p \equiv 3 \pmod{4}$ .

Voici comment ces formules conduisent aux intégrales (A) et (B).

J'observe d'abord que la formule connue

$$\frac{\Gamma(s)}{n^s} = \int_0^{\infty} x^{s-1} e^{-nx} dx$$

passât à l'expression suivante de la fonction  $\varphi(s)$

$$\varphi(s) = \frac{1}{\Gamma(s)} \int_0^\infty \frac{f(e^{-x})}{1 - e^{-px}} x^{s-1} dx.$$

Écrivant maintenant l'intégrale

$$\int_0^\infty \frac{f(e^{-x})}{1 - e^{-px}} \sin\left(\frac{ptx}{2\pi}\right) dx$$

à développer l'expression  $\sin\left(\frac{ptx}{2\pi}\right)$  suivant les puissances de  $x$

$$\sin\left(\frac{ptx}{2\pi}\right) = \frac{1}{\Gamma(2)} \left(\frac{ptx}{2\pi}\right) - \frac{1}{\Gamma(4)} \left(\frac{ptx}{2\pi}\right)^3 + \frac{1}{\Gamma(6)} \left(\frac{ptx}{2\pi}\right)^5 - \dots$$

En servant alors de la formule (1), l'intégrale se trouve égale à

$$\varphi(2) \left(\frac{pt}{2\pi}\right) - \varphi(4) \left(\frac{pt}{2\pi}\right)^3 + \varphi(6) \left(\frac{pt}{2\pi}\right)^5 - \dots$$

et sommer par la formule (C), ce qui fournit la formule (A).

La formule (B) s'obtient de la même manière à l'aide du développe-

ment qu'on vient de donner, ne s'applique directement  
seulement aux valeurs de  $t$  qui satisfont à la condition

$$\text{mod}(pt) < 2\pi$$

On a ainsi reconnu l'exactitude des formules (A) et (B) pour

les valeurs de  $t$  dont le module est inférieur à  $\frac{2\pi}{p}$ , on verra facilement

que ces formules sont valables pour une valeur imaginaire quelconque

$-bi$ , à condition seulement que la valeur absolue de  $b$  reste

inférieure à  $\frac{2\pi}{p}$ .

La fonction par laquelle nous avons défini la fonction  $\varphi(s)$  n'est con-

venue tant que la partie réelle de  $s$  est positive. Toutefois on

peut montrer que cette fonction est holomorphe dans tout le plan;

on le voit, en partant de la formule (1) et en suivant une méthode

de M. Hermite. (Comptes rendus de l'Acad. des Sciences,

p. 112).

Il existe une relation remarquable qui lie  $\varphi(s)$  à  $\varphi(1-s)$  et qui a été découverte par M. Hurwitz (*Zeitschrift für Mathematik und Physik*, tome 27, 1882). Sans avoir eu connaissance du travail de M. Hurwitz, j'avais retrouvé son résultat en partant des formules (A) et (B). Comme cette démonstration est entièrement différente de celle de M. Hurwitz, je crois utile de la donner ici. Je me bornerai d'ailleurs au cas  $p \equiv 1 \pmod 4$ .

En multipliant (A) par  $t^{s-1} dt$ , intégrant de 0 à  $\infty$  il vient, si l'on inverse l'ordre des intégrations dans l'intégrale double et qu'on se rappelle la relation connue :

$$\int_0^\infty \sin\left(\frac{p t x}{2\pi}\right) t^{s-1} dt = \Gamma(s) \left(\frac{p x}{2\pi}\right)^{-s} \sin \frac{\pi s}{2},$$

$$\Gamma(s) \sin \frac{\pi s}{p} \left(\frac{p}{2\pi}\right)^{-s} \int_0^\infty \frac{f(e^{-x})}{1 - e^{-p x}} x^{-s} dx = \frac{\pi}{\sqrt{p}} \int_0^\infty \frac{f(e^{-t})}{1 - e^{-p t}} t^{s-1} dt.$$

Or d'après (1)

$$\int_0^\infty \frac{f(e^{-x})}{1 - e^{-p x}} x^{-s} dx = \Gamma(1-s) \varphi(1-s),$$

$$\int_0^\infty \frac{f(e^{-t})}{1 - e^{-p t}} t^{s-1} dt = \Gamma(s) \varphi(s),$$

sorte qu'on trouve, après quelques réductions :

$$\varphi(1-s) = \left(\frac{p}{2\pi}\right)^s \frac{2 \cos \frac{\pi s}{2}}{\sqrt{p}} \Gamma(s) \varphi(s).$$

On peut dire aussi que l'expression

$$\left(\frac{p}{\pi}\right)^{\frac{s}{2}} \Gamma\left(\frac{s}{2}\right) \varphi(s)$$

change pas en remplaçant  $s$  par  $1-s$ .

Il faut supposer dans cette démonstration que  $s$  (ou la partie réelle de  $s$ ) reste comprise entre 0 et 1. Mais d'après le caractère analytique de la fonction  $\varphi(s)$ , la relation obtenue entre  $\varphi(s)$  et  $\varphi(1-s)$  doit avoir lieu dans tout le plan, dès qu'elle se trouve vérifiée dans une partie du plan.

remarque enfin que les formules que j'ai données dans ma communication déjà citée de Septembre 1885, permettent d'établir d'une manière beaucoup plus simple encore cette relation entre  $\varphi(s)$  et  $\varphi(1-s)$ . Riemann, dans le mémoire cité, a donné une relation entre la fonction qu'il désigne par  $\zeta(s)$  et  $\zeta(1-s)$ , et il a démontré cette propriété de deux manières différentes, la seconde démonstration se fondant sur une formule qui appartient à la théorie des fonctions elliptiques. La démonstration de la relation qui lie  $\varphi(s)$  à  $\varphi(1-s)$  que nous venons d'établir en dernier lieu, est parfaitement analogue à cette seconde démonstration de Riemann.

Il n'est pas sans intérêt d'examiner un peu plus particulièrement les développements en série (C) et (D).

Il est évident d'abord que les coefficients des diverses puissances de  $x$  dans le développement de

$$\frac{f(e^{-x})}{1 - e^{-px}} = \frac{e^{\frac{p}{2}x} f(e^{-x})}{e^{\frac{p}{2}x} - e^{-\frac{p}{2}x}}$$

pour des nombres rationnels; en égalant ces nombres aux expressions qui figurent dans les seconds membres de (C) et de (D) on obtient les coefficients des séries infinies  $\varphi(1)$ ,  $\varphi(2)$ ,  $\varphi(3)$ , etc. Ces sommations méritent d'être mises à côté des formules bien connues qui expriment les sommes des séries

$$\frac{1}{1^{2n}} + \frac{1}{2^{2n}} + \frac{1}{3^{2n}} + \frac{1}{4^{2n}} + \dots,$$

$$\frac{1}{1^{2n-1}} - \frac{1}{3^{2n-1}} + \frac{1}{5^{2n-1}} - \frac{1}{7^{2n-1}} + \dots$$

$$e^{\frac{p}{2}x} f(e^{-x}) = \sum_{n=1}^{p-1} \left(\frac{n}{p}\right) e^{\frac{p-2n}{2}x}.$$

En distinguant les deux cas  $p \equiv 1$ ,  $p \equiv 3 \pmod{4}$  et en posant  $p' = \frac{p-1}{2}$

$$x^{p-1} = \sum_{j=0}^{p-1} \binom{n}{j} (x^{\frac{p-1}{2}-jn} + x^{\frac{p-1}{2}+jn}) \quad p \equiv 1 \pmod{4},$$

$$x^{p-1} = \sum_{j=0}^{p-1} \binom{n}{j} (x^{\frac{p-1}{2}-jn} - x^{\frac{p-1}{2}+jn}) \quad p \equiv 3 \pmod{4},$$

on

$$\begin{aligned} \sum_{j=0}^{p-1} \binom{n}{j} \frac{1}{j!} \left( \frac{p-2n}{2} \right)^j x^j + \frac{1}{1.2.3.4} \left( \frac{p-2n}{2} \right)^4 x^4 + \dots \\ 1 - x^{p-1} = \frac{p}{2} + \frac{1}{1.2.3} \left( \frac{p}{2} \right)^3 x^3 + \frac{1}{1.2.3.4.5} \left( \frac{p}{2} \right)^5 x^5 + \dots \\ p \equiv 1 \pmod{4} \end{aligned}$$

$$\begin{aligned} \sum_{j=0}^{p-1} \binom{n}{j} \frac{p-2n}{2} x + \frac{1}{1.2.3} \left( \frac{p-2n}{2} \right)^3 x^3 + \dots \\ 1 - x^{p-1} = \frac{p}{2} + \frac{1}{1.2.3} \left( \frac{p}{2} \right)^3 x^3 + \frac{1}{1.2.3.4.5} \left( \frac{p}{2} \right)^5 x^5 + \dots \\ p \equiv 3 \pmod{4}. \end{aligned}$$

La comparaison avec les développements (C) et (D) donne une série formules dont les premières et les plus simples peuvent s'écrire

$$\frac{1}{2p} \sum_{j=1}^{p-1} \binom{n}{j} n^j = \frac{p-1}{2} \quad p \equiv 1 \pmod{4},$$

$$\frac{1}{p} \sum_{j=1}^{p-1} \binom{n}{j} n^j = \frac{p-1}{2} \quad p \equiv 3 \pmod{4},$$

on

$$\sum_{j=1}^{p-1} \binom{n}{j} \frac{1}{j!} = \frac{n^2}{p!} \sum_{j=1}^{p-1} \binom{n}{j} n^j \quad p \equiv 1 \pmod{4},$$

$$\sum_{j=1}^{p-1} \binom{n}{j} \frac{1}{j!} = \frac{n^2}{p!} \sum_{j=1}^{p-1} \binom{n}{j} n^j \quad p \equiv 3 \pmod{4}.$$

La formule (A) s'est présentée déjà à Dirichlet dans ces célèbres recherches sur la détermination du nombre des classes des formes quadratiques à deux indéterminées, le cas le plus simple  $p=3$

$$\frac{1}{3!} 3^3 = 1 - \frac{1}{2} + \frac{1}{4} - \frac{1}{6} + \frac{1}{7} - \frac{1}{8} + \dots$$

trouve dans l'Introduction in Analysis infinitorum d'Euler (§ 176).